**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ЮРИДИЧНИЙ ФАКУЛЬТЕТ**

кафедра цивільного права

(повна назва кафедри)

**Кваліфікаційна робота**

магістр

(рівень вищої освіти)

на тему Міжнародно-правові стандарти у сфері забезпечення міжнародної інформаційної безпеки

Виконав: слухач магістратури, групи 8.2629-1з

спеціальності

262 Правоохоронна діяльність

(шифр і назва спеціальності)

|  |
| --- |
| Правоохоронна діяльність |

(назва освітньої програми)

Д.А.Кравченко

(ініціали та прізвище)

Керівник доцент, к.ю.н. Луц Д.М.

(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент зав.каф., д.ю.н., професор

Єрмоленко Д.О.

(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя – 2020

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

Факультет юридичний                                        \_\_

Кафедра цивільного права \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рівень вищої освіти магістр

Спеціальність 262 Правоохоронна діяльність

(шифр і назва)

Освітня програма Правоохоронна діяльність

**ЗАТВЕРДЖУЮ**

Завідувач кафедри\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_року

**З А В Д А Н Н Я**

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТЦІ

Кравченку Дмитру Анатолійовичу

(прізвище, ім’я, по батькові)

1. Тема роботи (проекту) Міжнародно-правові стандарти у сфері забезпечення міжнародної інформаційної безпеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

керівник роботи Луц Дмитро Миколайович, к.ю.н., доцент

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від «14» травня 2020 року № 554-с

1. Строк подання роботи 05 листопада 2020 року
2. Вихідні дані до роботи нормативно-правові акти, наукові публікації,\_\_\_\_\_\_ підручники, посібники, довідники, монографії
3. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) поняття, ознаки, проблеми реалізації, перспективи формування
4. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

схеми, таблиці

6. Консультанти розділів роботи

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  консультанта | Підпис, дата | |
| завдання  видав | завдання  прийняв |
| 1 | Луц Д.М., к.ю.н., доцент |  |  |
| 2 | Луц Д.М., к.ю.н., доцент |  |  |

1. Дата видачі завдання травень 2020 року

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №  з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
| 1. | Обрання та затвердження теми | травень 2020 | виконано |
| 2. | Складання плану роботи | травень 2020 | виконано |
| 3. | Пошук та оформлення наукових джерел, нормативно-правової бази | червень 2020 | виконано |
| 4. | Написання реферату українською та англійською мовами | липень 2020 | виконано |
| 5. | Пояснювальна записка | серпень 2020 | виконано |
| 6. | Написання практичної частини | вересень 2020 | виконано |
| 7. | Висновки | жовтень 2020 | виконано |
| 8. | Попередній захист кваліфікаційної роботи | листопад 2020 | виконано |
| 9. | Захист кваліфікаційної роботи |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Слухач \_\_\_\_\_\_\_\_\_\_\_\_\_Кравченко Д.А

(підпис) (ініціали та прізвище)

Керівник роботи (проекту) \_\_\_\_\_\_\_\_\_\_\_\_\_Д.М. Луц

(підпис) (ініціали та прізвище)

**Нормоконтроль пройдено**

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_ Ш.М. Гаджиєва

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Кравченко Д.А. Міжнародно-правові стандарти у сфері забезпечення міжнародної інформаційної безпеки – Запоріжжя, 2020. – 125 с.

Кваліфікаційна робота складається зі 125 сторінок, містить 71 джерело використаної інформації.

В умовах євроінтеграції України, з урахуванням побудови інформаційного суспільства, все більшої актуальності набувають питання правового забезпечення інформаційної безпеки – запобігання й усунення різноманітними засобами і способами загроз людині, суспільству, державі в інформаційній сфері. Однак у сучасному багатогранному та динамічному світі проблеми інформаційної безпеки набувають принципово нових рис, тепер вони виходять далеко за межі запобігання війн і збройних конфліктів. Сьогодні вони стали їх підґрунтям, першоджерелом, основним ресурсом та головною зброєю.

За нинішніх обставин стратегічного значення набуває удосконалення існуючих та створення нових механізмів взаємодії в інформаційному сегменті національної безпеки між інститутами та організаціями громадянського суспільства, з однієї сторони, та державною владою і органами місцевого самоврядування, з іншої, з метою своєчасного виявлення, попередження та нейтралізації наявних та потенційних інформаційних загроз.

Своєчасність теми роботи зумовлюється передовсім гостротою самої проблеми забезпечення інформаційної безпеки, особливо її правового складника, сфокусованого на забезпеченні безпеки людини, суспільства й держави.

Мета роботи полягає у встановленні сутності та особливостей міжнародно-правових стандартів у сфері забезпечення інформаційної безпеки, їх правового базису та теоретичного забезпечення.

Об’єктом кваліфікаційної роботи є суспільні відносини в області міжнародно-правових стандартів у сфері забезпечення інформаційної безпеки.

Предмет кваліфікаційної роботи – особливості міжнародно-правових стандартів у сфері забезпечення інформаційної безпеки.

Методологічною основою роботи є сукупність принципів, загальнонаукових і спеціально-галузевих методів правового пізнання. В процесі дослідження використовувались положення сучасної теорії пізнання і загальної теорії міжнародно-правових стандартів. Основні висновки ґрунтуються на методі системного аналізу міжнародно-правових стандартів, практики їх застосування; формально-логічний, логіко-юридичний та порівняльно-правовий методи застосовувались під час дослідження правових норм щодо вдосконалення криміналістичної методики розслідування масових заворушень; історичний – при дослідженні появи і розвитку окремих теорій, концепцій, поглядів вчених з проблем розробки міжнародно-правових стандартів у сфері забезпечення міжнародної інформаційної безпеки; системно-структурний – під час аналізу особливостей формування міжнародно-правових стандартів у сфері забезпечення міжнародної інформаційної безпеки; системно-аналітичний – для опрацювання офіційних, наукових та бібліографічних джерел, збору та узагальнення думки практичних працівників і науковців у процесі створення фактологічного підґрунтя предмету роботи.

БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНЕ ПРАВО, ІНФОРМАЦІЙНІ ПРАВОВІДНОСИНИ, ЗАГРОЗИ, ІНФОРМАЦІЙНА ПОЛІТИКА, КІБЕРБЕЗПЕКА, КІБЕРЗАГРОЗИ, СТАНДАРТИ ІНФОРМАЦІЇ БЕЗПЕКИ

summary

Kravchenko D.A. International legal standards in the field of international information security - Zaporozhye, 2020. - 125 р.

Qualification work consists of 125 pages containing 71 sources of information used.

In the context of Ukraine's European integration, taking into account the construction of the information society, the issues of legal support of information security - prevention and elimination by various means and methods of threats to man, society, state in the information sphere are becoming increasingly important. However, in today's multifaceted and dynamic world, information security problems are acquiring fundamentally new features, now they go far beyond the prevention of wars and armed conflicts. Today, they have become their foundation, primary source, main resource and main weapon.

In the current circumstances, it is of strategic importance to improve existing and create new mechanisms of interaction in the information segment of national security between civil society institutions and organizations, on the one hand, and public authorities and local governments, on the other, to identify, prevent and neutralize existing and potential information threats.

The timeliness of the topic of work is determined primarily by the severity of the problem of information security, especially its legal component, focused on ensuring the security of man, society and the state.

The purpose of the work is to establish the essence and features of international legal standards in the field of information security, their legal basis and theoretical support.

The object of the qualification work is public relations in the field of international legal standards in the field of information security.

The subject of qualification work - features of international legal standards in the field of information security.

The methodological basis of the work is a set of principles, general scientific and special-branch methods of legal knowledge. In the course of the research the provisions of the modern theory of cognition and the general theory of international legal standards were used. The main conclusions are based on the method of systematic analysis of international legal standards, the practice of their application; formal-logical, logical-legal and comparative-legal methods were used during the study of legal norms to improve forensic methods of investigating mass riots; historical - in the study of the emergence and development of individual theories, concepts, views of scientists on the development of international legal standards in the field of international information security; system-structural - during the analysis of the peculiarities of the formation of international legal standards in the field of international information security; system-analytical - for the elaboration of official, scientific and bibliographic sources, collection and generalization of the opinion of practical workers and scientists in the process of creating the factual basis of the subject of work.

SECURITY, INFORMATION SECURITY, INFORMATION LAW, INFORMATION LEGAL RELATIONS, THREATS, INFORMATION POLICY, CYBER SECURITY, CYBER SECURITY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ………….....…...........................................9

РОЗДІЛ 1. ПОЯСНЮВАЛЬНА ЗАПИСКА……................................................10

РОЗДІЛ 2. ПРАКТИЧНА ЧАСТИНА…………………………………………..40

2.1 Визначення поняття безпеки………………………….……………...40

2.2 Визначення поняття інформації……………...………………………46

2.3 Визначення поняття інформаційної безпеки …………...…………..55

2.4 Визначення поняття міжнародно-правових стандартів …………....59

2.5 Міжнародна інформаційна безпека ……………………………...….73

2.6 Правове забезпечення розвитку інформаційного суспільства:

Окінавська Хартія глобального інформаційного суспільства ………...76

2.7 Конвенція про кіберзлочинність …………………………….………89

ВИСНОВКИ………….........................................................................................116

ПЕРЕЛІК використаних джерел…………….......................................119

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРУ Верховна Рада України

Європейський Союз ЄС

Засоби масової інформації ЗМІ

Інформаційна безпека ІБ

Інформаційна зброя ІЗ

Інформаційно-комунікаційні технології ІКТ

Інформаційно-психологічний вплив ІПВ

КК Кримінальний кодекс

КМУ Кабінет Міністрів України

КУ Конституція України

Міністерство оборони МО

Національна безпека НБ

НПА нормативно-правовий акт

п. пункт

р. рік

Служба безпеки України СБУ

ст. стаття

РОЗДІЛ 1 ПОЯСНЮВАЛЬНА ЗАПИСКА

*Актуальність теми*. В умовах євроінтеграції України, з урахуванням побудови інформаційного суспільства, все більшої актуальності набувають питання правового забезпечення інформаційної безпеки – запобігання й усунення різноманітними засобами і способами загроз людині, суспільству, державі в інформаційній сфері. Однак у сучасному багатогранному та динамічному світі проблеми інформаційної безпеки набувають принципово нових рис, тепер вони виходять далеко за межі запобігання війн і збройних конфліктів. Сьогодні вони стали їх підґрунтям, першоджерелом, основним ресурсом та головною зброєю.

Зважаючи на тему роботи, очевидно, що для України має велике значення опрацювання досвіду забезпечення міжнародної інформаційної безпеки, в українських реаліях ці проблеми стали очевидними у 2014 році з подальшою ескалацією конфлікту. У таких умовах стає пріоритетним осмислення сукупності інформаційних процесів у контексті правового забезпечення безпеки України. З огляду на це цілком природним вбачається пошук основоположних цінностей, цілей, інтересів та надбань в інформаційній сфері, які слугуватимуть орієнтирами європейської перспективи України, майбутнього розвитку українського суспільства, заснованої на інформаційних технологіях, закладуть фундамент подальшого розвитку інформаційного права в Україні.

У цьому контексті закономірно зростає роль правових механізмів у забезпеченні інформаційної безпеки України і світу, потреба ефективного законодавчого врегулювання суспільних відносин, що виникають у досліджуваній сфері, визначення правових засад організації та координації дій суб’єктів забезпечення інформаційної безпеки, розробці пріоритетних напрямів державної політики у сфері інформаційної безпеки. Дослідження інформаційної безпеки з правничої точки зору пов’язане з формуванням якісної системи інформаційної безпеки, що відповідатиме сучасним вимогам та нагальним потребам України як повноправного члена й надійного партнера європейської спільноти.

Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері. Для нашої держави імплементація європейських стандартів правового забезпечення інформаційної безпеки держави є пріоритетним засобом інтеграції в європейський правовий простір.

За нинішніх обставин стратегічного значення набуває удосконалення існуючих та створення нових механізмів взаємодії в інформаційному сегменті національної безпеки між інститутами та організаціями громадянського суспільства, з однієї сторони, та державною владою і органами місцевого самоврядування, з іншої, з метою своєчасного виявлення, попередження та нейтралізації наявних та потенційних інформаційних загроз. Отже, мають важливе значення наукові пошуки підвищення ефективності державно-громадської взаємодії та використання потенціалу громадського сектору у протидії сучасним викликам інформаційній безпеці.

Актуальність теми роботи зумовлюється передовсім гостротою самої проблеми забезпечення інформаційної безпеки, особливо її правового складника, сфокусованого на забезпеченні безпеки людини, суспільства й держави.

Дослідження даної теми важливе для розуміння специфіки інформаційної безпеки та її потужного впливу на подальший розвиток суспільства.

Підсилює актуальність дослідження необхідність розширення можливостей участі громадського сектору у процесах підготовки та ухвалення політико-управлінських рішень у безпековому секторі, формуванні та реалізації національної безпеки в інформаційній сфері. До того ж, комплексний аналіз процесу забезпечення національної безпеки на рівні недержавної (суспільної) системи актуалізується в контексті дії низки зовнішньо-та внутрішньополітичних чинників, які підсилюють деструктивні суспільно-політичні процеси.

*Об’єктом кваліфікаційної роботи* є суспільні відносини в області міжнародно-правових стандартів у сфері забезпечення інформаційної безпеки.

*Предмет кваліфікаційної роботи* – особливості міжнародно-правових стандартів у сфері забезпечення інформаційної безпеки.

*Мета* роботи полягає у встановленні сутності та особливостей міжнародно-правових стандартів у сфері забезпечення інформаційної безпеки, їх правового базису та теоретичного забезпечення.

Зазначені мета та об’єкт роботи зумовили наступні *завдання* дослідження, які мають бути вирішені в роботі:

– дослідити генезис наукових поглядів у сфері правового забезпечення інформаційної безпеки;

– на основі понятійно-категоріального синтезу з’ясувати змістовну сутність основних понять, пов’язаних із інформаційної безпекою;

– охарактеризувати методологічні засади міжнародно-правової стандартизації в сфері забезпечення інформаційної безпеки;

– з’ясувати місце правового забезпечення інформаційної безпеки України у системі інформаційного права;

– класифікувати складові елементи в системі інформаційної безпеки;

– визначити теоретичні підходи до змісту загроз інформаційній безпеці;

– узагальнити досвід правового забезпечення політики інформаційної безпеки Північноатлантичного альянсу.

*Ступінь наукової розробки* проблеми. Основним теоретичним підґрунтям дисертаційної роботи стали пов’язані з проблематикою даного дослідження праці в таких галузях та таких вчених:

філософії: А. Бергсон, Г. Гроцій, Р. Ієрінг, Н. Макіавеллі, Р. Оуен, Плутарх, Платон, Б. Рассел, Сенека, Сунь-цзи, А. Сен-Сімон;

інформаційного права: І. Арістова, О. Баранов, К. Бєляков, В. Брижко, І. Бондар, С. Бондаренко, О. Довгань, С. Домбровська, М. Згуровський, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, О. Костенко, В. Клочко, О. Логінов, В. Ліпкан, А. Марущак, Є. Мануйлов, О. Морозов, А. Нашинець-Наумова, В. Остроухов, І. Панова, В. Пилипчук, В. Петрик, В. Політанський, М. Присяжнюк, Ю.Размєтаєва, В. Рубан, Ю. Руденко, Г. Сащук, Я.Собків, О. Тихомиров, В. Фурашев, С. Феденько, Л. Харченко, О. Хілько, В. Шамрай, Р. Шаповал, В. Шатун, О. Ярема та ін.

інших галузей права: вітчизняні вчені – Ю. Бисага, Д. Бєлов, О. Береза, Ю. Білак, В. Білоус, В. Горбулін, В. Григор’єв, В. Гулай, О. Дзьобань, Т. Карабін, А. Качинський, Я. Лазур, А. Легеза, Ю. Лісовська, І. Лях, Я. 31 Малик, Й. Мастяниця, С. Мельник, Н. Нижник, Д. Прокоф’єва-Янчиленко, Г. Ситник, М. Савчин, О. Соснін, Л. Шиманський; зарубіжні вчені: С. Алексєєв, Дж. Барбер, Н. Вінер, В. Герхард, К. Геерс, Дж. Данн, К. Демпсі, Л. Козер, П. Корніш, А. Кемпф Р. Оуен, В. Пілліттері, Б. Рассел, А. Робертс, Ф. Сталдер, М. Лібіскі, О. Лукашов, А. Левін, Х. Міллінгтон, М. Нільес, К. Шенон, К. Шилде, Р. Ярґер та ін.

Опис проблеми, що досліджується. Коли йдеться про інформаційно-комунікаційні технології, передовсім маються на увазі засоби зв’язку чи, швидше, канали зв’язку. З найдавніших часів зв'язок асоціювався з магією. Одним з різновидів магії був звук. Людський голос (звук, який видається людиною) вважався магічним за своєю природою. У книзі Буття Адам виконував магічну за своєю суттю дію, даючи наймення рослинам і тваринам. Таким чином він підтверджував дану йому Богом могутність, а проголошення назв стало справжньою демонстрацією магічних можливостей. Самі імена теж наділялися магічною силою. Так, у древньому іудаїзмі ім’я Бога само по собі було ототожненням могутності, а промовляти його міг лише первосвященик раз на рік, перебуваючи наодинці у найсвятішій частині Храму. У багатьох культурах особи, які проходили певні ритуали посвячення, отримували нові й часто втаємничені імена. За давньою ірландською легендою поет, котрий мав магічну здатність управляти мовою, міг проклясти будь-яку людину, давши їй ім’я із «вплетеним» у нього прокляттям.

Чим менш доступними були засоби зв’язку, перетворюючись на прерогативу посвячених, тим більше вони асоціювалися з таємницею та магією. Відомо, що німецький гуманіст, лікар, алхімік, натурфілософ, окультист, астролог і знаний адвокат Агріппа листувався з ученими інших країн, а пізніше зміцнював свій імідж мага, видаючи отриману від них інформацію за повідомлення духів.

Абсолютно не принципово, що наш розум сьогодні звик сприймати ці речі як продукти технології, а не магії. До того як картезіанське мислення призвело до фрагментації знання, магія і технології були єдині. Нині вони залишаються нероздільними лишень у метафоричному сенсі. Проте, незалежно від термінології, багато хто й донині продовжує говорити про «мистецтво створювати події». До нас пройшло дуже багато часу. Змінися й технології. Ми живемо в епоху цифрових технологій і вже не уявляємо нашого буття без Інтернету, електронної пошти та інших плодів технологічного прогресу. Проте і сьогодні, як сказав колись Уїнстон Черчіль, «хто володіє інформацією, той володіє світом». Тобто володіння інформацією залишається певним магічним дійством, здатним впливати на маси, результати парламентських чи президентських виборів, ставати збудником революцій, війн і т.д. І якщо цей світ являє собою найбільш яскраву на сьогодні демонстрацію магічної сили, то він також є потужною потенційною силою для маніпуляцій свідомістю, а це і є своєрідною магією. Якщо ж відбуваються якісь впливи на поведінку людини чи груп людей, логічно постає й категорія «безпеки», котра в цьому разі матиме дуалістичну характеристику: безпека інформації як інструменту впливу та безпека від інформації, яка може вплинути. В обох випадках суб’єктний склад різний.

У XVI столітті італійські мислителі сформулювали інформаційно-психологічну концепцію державної влади, де виклали основні принципи інформаційного протиборства в політичній сфері. Крім того, історія багата прикладами проведення потужних інформаційно-пропагандистських акцій, класичних варіантів глобальної дезінформації народу, які відіграли свою фатальну роль.

Багато цікавих ідей щодо вирішення безпекових проблем висунули соціалісти-утопісти, французькі мислителі, соціологи, засновники утопічного соціалізму - запропонував ідею своєрідної колективної безпеки народів. Вважали, що філософська система, котру назвали «новим християнством», «оновленою релігією», є інформаційним підґрунтям, покликаним «створити для всіх народів стан вічного миру й безпеки, об’єднуючи їх проти тієї нації, яка побажала би досягти свого власного блага за рахунок загального блага всього людства. Таке досягнення здійснюється шляхом об’єднання їх (народів) проти всякого уряду, який пройнятий антихристиянським духом до такої міри, щоб загальнонаціональні інтереси принести в жертву приватним інтересам правителів». Очевидно, що така ідея, як на той час, так і сьогодні, не є обґрунтованою і для наукового аналізу серйозно сприйматися не може.

Мислителі різних епох засуджували насильство, пристрасно мріяли про вічний мир і безпеку, пропонували різні моделі здійснення своїх задумів. Одні з них звертали увагу насамперед на інформаційно-етичний бік проблеми. Вони вважали, що агресія, війна є породженням аморальності, що безпечного стану можливо досягти тільки шляхом морального перевиховання людей у дусі взаєморозуміння, терпимості до різних віросповідань, усунення націоналістичних пережитків, виховання людей за принципом «усі люди - брати». Інші вбачали головну перешкоду для досягнення безпечного суспільного стану в господарській руїні, в порушенні нормального функціонування всієї економічної та інформаційної структур, у колізії природного й громадянського станів особистості. У зв’язку з цим вони намагалися схилити людство до миру й безпеки, малюючи картини загального процвітання в суспільстві без воєн, у якому пріоритет надаватиметься розвитку науки, техніки, мистецтва, літератури, інформації, а не вдосконаленню засобів знищення. Вони вважали, що міждержавну безпеку можна встановити завдяки розумній політиці освіченого правителя. Треті розробляли правові аспекти безпеки, досягти якої вони пропонували шляхом угоди між урядами, створенням регіональних або всесвітніх федерацій держав. Четверті переконували, що коріння небезпек має соціальний характер, що усунути їх можна, лише змінивши структуру суспільства.

Нині у глобальному медіапросторі, в публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн широкого вжитку набули терміни «інформаційна війна», «інформаційне протиборство», «інформаційний вплив», «інформаційна зброя» тощо. Інформаційно-комунікаційні технології відіграють ключову роль у світовій політиці, економіці та системах безпеки. До інформаційних диверсій у кіберпросторі сьогодні вдаються як організовані групи, так і окремі особи. Дедалі важливішою складовою військового потенціалу держав стає інформаційна зброя як доповнення до власне військового арсеналу. При цьому за своїми наслідками інформаційні війни між державами можуть бути не менш руйнівними і жорстокими, ніж традиційні. Утім, і в давні часи психологічна перевага над ворогом подеколи була важливішою за його фізичне знищення.

Доба глобальної інформаційної революції значно розширила можливості для подібної діяльності. Мабуть, першим прикладом використання ІКТ у ході бойових дій стала операція «Буря в пустелі», проведена Сполученими Штатами Америки в Іраку в 1991 році. Новітній формат протистояння передбачав тривалий інформаційно-психологічний тиск і комплексне застосування засобів розвідки, управління, зв’язку, навігації та радіоелектронної боротьби. З кінця 1990-х років спостерігається послідовне зростання потужності інформаційних впливів у рамках операцій у Югославії (1999), Афганістані (2001), Іраку (2003), Лівії (2011); 2008 року під час збройного конфлікту в Грузії дієвий деструктивний інформаційно-психологічний вплив забезпечили західні держави. Наразі у протистояннях в Україні та Сирії реалізуються майже всі наявні методи інформаційного впливу.

При цьому на міжнародному рівні дотепер відсутні загальноприйняті визначення терміну «інформаційно-комунікаційні технології» і пов’язаних з ним понять. Процес юридичного оформлення понятійного апарату сфери ІКТ у глобальному правовому просторі триває, і, оскільки метою спільних зусиль у зазначеному напрямі є узгодження численних термінологічних суперечностей, важливо простежити розвиток відповідної термінології в національних державних документах. З-поміж широкого спектра понять, прямо й опосередковано пов’язаних з проблематикою інформаційної безпеки, у цій роботі зосередимося лише на тих, що є найбільш значущими для її теми.

Дослідники питань інформаційної безпеки особливу увагу приділяють такому поняттю, як «інформаційна війна». Уперше цей термін використав науковий радник Міністерства оборони Сполучених Штатів у звіті «Системи зброї та інформаційної війни», який він підготував у 1976 році для компанії «Боїнг» . У цьому документі висловлюється думка, що інформаційна інфраструктура як ключова складова економіки США стає вразливою ціллю як у воєнний, так і в мирний час. В офіційний обіг термін «інформаційна війна» ввів міністр оборони США в директиві від 21.12.1992 «Інформаційне протиборство» («Information Warfare»). Отже, збройні сили Сполучених Штатів першими використали новітні інформаційні технології у війні в Перській затоці (1991), а після її завершення ключові персони військової сфери США, знову ж таки першими на світовій арені, на офіційному рівні сформулювали стратегічні засади інформаційного протиборства.

У серпні 1995 року була оприлюднена його стаття «Що таке інформаційна війна?». Пізніше писали, що психологічний вплив на противника під час військових дій використовується з давніх часів, проте у війнах нашої доби технічні методи і психологічні інформаційні операції мають однаково важливе значення й застосовуються в комплексі. Науковці пропонували одну з перших класифікацій інформаційних воєн. Вони виокремили сім різних аспектів цього феномена:

1) війна у сфері контролю та управління;

2) розвідувальна війна;

3) електронна війна;

4) психологічна війна;

5) хакерська війна;

6) економічна інформаційна війна;

7) кібервійна.

На реальному полі бою ведеться війна у сфері контролю та управління, спрямована на переривання каналів зв’язку між командуванням і виконавцями. Цей вид активності нападника має на меті порушення систем управління військами, ліній комунікацій і системи управління противника в цілому на стратегічному, оперативному й тактичному рівнях. У кінцевому підсумку сторона, що атакує, прагне домогтися цілковитої ізоляції командування від виконавців.

Метою економічної інформаційної війни вважають комерційну інформацію, припускаючи, що замість залежності держав від матеріального забезпечення й обміну прийде дедалі більша залежність від інформаційних потоків. Двома основними формами такої війни є інформаційна блокада та інформаційний імперіалізм.

Особливість сучасного розвитку суспільних відносин в Україні полягає в тому, що становлення української державності відбувається паралельно, в умовах проголошення курсу на інтеграцію до Європейського Союзу, що сприяє системному реформуванню всіх галузей права відповідно до законодавства ЄС. Проте, при реалізації європейських планів виникає низка питань щодо вдосконалення правового регулювання інформаційних відносин. З-поміж цих питань, наприклад: розвиток масивів відкритих даних органів державної влади, адже відкриття даних змінює підходи до державного управління та стратегічного розвитку України; системи відкритих даних органів місцевого самоврядування; колізії щодо захисту даних від протиправних посягань; електронне врядування та ін.

8 червня 2017 року було прийнято Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України», яким внесено зміни до законів України «Про національну безпеку України» та «Про засади внутрішньої і зовнішньої політики» у частині євроатлантичної інтеграції. Одним із пріоритетів національних інтересів України цим законом визначено інтеграцію у євроатлантичний безпековий простір з метою набуття членства в Організації Північноатлантичного договору. Остаточно обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку країн Європи в інформаційній сфері. Найбільш успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства є країни Європи, що входять до НАТО.

Зазначені зміни в законодавстві свідчать про поглиблення співпраці України з НАТО задля набуття членства в цій організації. За таких умов набуває все більшого значення координація діяльності органів виконавчої влади, ЗМІ тощо з питань співробітництва з НАТО в інформаційній сфері. Цей вектор розвитку зовнішньої політики України впливає й на правове регулювання системи безпеки інформації як складової частини євроатлантичного безпекового простору, що, у свою чергу, потребує глибокого розуміння сутності політики інформаційної безпеки НАТО та інформаційної політики Альянсу в цілому.

Досліджуючи питання політики інформаційної безпеки НАТО в сучасних умовах, слід передусім з’ясувати сутність інформаційної політики цієї організації в цілому, а також питання забезпечення безпеки інформації та кібербезпеки у системі Альянсу.

Наразі регулювання інформаційної сфери у країнах НАТО здійснюється за такими напрямами:

1) заохочення конкуренції, боротьба з монополізмом та концентрацією ЗМІ;

2) забезпечення права і технічних можливостей для доступу до інформації та інформаційних ресурсів усього населення;

3) дотримання свободи слова;

4) захист інтересів національних меншин, національної культурної спадщини, мови, протистояння культурній експансії інших країн; захист молоді в інформаційній сфері;

5) охорона інтелектуальної власності, боротьба з піратством;

6) протидія кіберзлочинності; впровадження електронного урядування;

7) правове регулювання мережі Інтернет;

8) забезпечення інформаційної безпеки тощо.

Система інформаційної політики НАТО є похідною від реалізації демократичного принципу цивільного контролю над військово-політичною сферою в умовах участі громадськості в міжнародному військово-політичному процесі. З підвищенням суспільного інтересу до діяльності Альянсу на початку 1990-х років основна роль у провадженні інформаційної діяльності відводиться власним інститутам НАТО. Основним органом проведення інформаційної політики організації є Атлантична рада, яка оприлюднює свої рішення й заяви для преси та широкого загалу. Крім Атлантичної ради, інформуванням громадськості опікуються установи країн-членів НАТО.

Одну із провідних ролей у реалізації інформаційної політики Альянсу відіграє Бюро інформації та преси. Воно входить до числа структур відділу Генерального секретаря (після празького саміту 2002 року його функції виконує Департамент публічної дипломатії, який забезпечує інформаційну діяльність). У ході реалізації різних програм і заходів Бюро інформації та преси сприяє урядам країн-членів і держав-партнерів у розширенні розуміння громадськістю ролі й напрямків політики НАТО. Бюро підтримує тісні зв’язки з національними інформаційними органами й неурядовими організаціями та здійснює заходи, спрямовані на роз’яснення громадськості цілей, завдань і досягнень НАТО.

Якщо вести мову про забезпечення безпеки інформації, то слід зазначити, що при створенні НАТО в 1949 році системи безпеки країн-учасниць істотно різнилися. Перша натівська система засекречування містила вісім рівнів таємності, була розроблена для документів у вигляді «твердих копій», а також передбачала створення в кожній країні двох центральних режимних органів і певну кількість підпорядкованих їм структур. На початку 1990-х років НАТО розпочала політичну та військову трансформацію структур безпеки, відчувши не тільки позитивні (скорочення часу обміну, збільшення місткості носіїв, швидкість пошуку, класифікацію, створення баз даних), а й негативні (втрата конфіденційності, цілісності змісту інформації або цілісності системи, втрата доступу) наслідки інформатизації. Виникнення нових загроз у сфері інформаційної безпеки зумовило необхідність осучаснення підходів до забезпечення безпеки інформації.

Засади політики НАТО щодо забезпечення безпеки так званої класифікованої інформації викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)». Класифікована інформація - термін, який використовується у законодавстві країн−членів НАТО стосовно частини «уразливої» (sensitive) інформації, тобто інформації, чутливої до загроз, що виникають у зв’язку з несанкціонованим доступом до неї, а тому потребує захисту або принаймні обмеження доступу до неї. НАТО має п’ять рівнів захисту інформації з обмеженим доступом: Сosmic TOP Secret, NАТО Secret, NАТО Сonfidential, NАТО Restricted, Unclassified but Sensitive. При цьому, у внутрішньодержавному законодавстві застосовують не більше трьох рівнів класифікації для інформації з обмеженим доступом, враховуючи інформацію з грифом, що відповідає рівню RESTRICTED і належить до офіційної, службової та громадської публічної таємниці. Певні термінологічні та сутнісні розбіжності у визначенні та класифікації інформації з обмеженим доступом в національному законодавстві країн НАТО компенсуються уніфікацією підходів до такої інформації у базових сферах діяльності держав-членів – військовій, економічній, правоохоронній та ін.

Документ СМ (2002)49 встановлює основні вимоги до системи забезпечення фізичної, організаційної, процедурної та технічної безпеки, зокрема й безпеки інформації. Дотримуючись спільних зобов’язань, кожна країна-член НАТО надає інформації з обмеженим доступом власну оцінку, і, залежно від того, як інші члени виконують прийняті на себе зобов’язання, визначає, яку саме інформацію зробити доступною Альянсу. Відтак, будь-яке відхилення одного чи декількох членів Альянсу від виконання їхніх зобов’язань може призвести до скорочення обсягу та якості переданої їм інформації. Зазначений документ проголошує п’ять основних принципів політики безпеки НАТО:

1) широти;

2) глибини;

3) централізації;

4) управління доступом;

5) персонального контролю

Засадничим принципом безпеки інформації в системі НАТО є при цьому те, що інформація має зберігати свій ступінь захисту протягом усього циклу її обігу, починаючи від джерела. При цьому контроль за розподілом і поширенням інформації має унеможливити її витік.

Завдання, які пов’язані із забезпеченням захисту інформації входять до компетенції Комітету внутрішньої безпеки НАТО. Даний Комітет є дорадчим органом при Північноатлантичній Раді з питань, що стосуються безпеки НАТО. Усередині НАТО національний уповноважений орган з безпеки інформації виконує функції керівництва створенням органу правління та режимних відділів, забезпечення безпеки таємної інформації НАТО в усіх установах, що перебувають під її юрисдикцією, як усередині країни, так і за її межами, забезпечення розробки планів захисту інформації в разі виникнення надзвичайних обставин з метою запобігання втрати конфіденційності інформації НАТО. Представники національного уповноваженого органа із забезпечення безпеки інформації беруть участь у нарадах Комітету безпеки НАТО, де виробляються політика й інструкції у безпековій сфері. На обсяг функцій відповідального уповноваженого впливають розмір і кількість населення країни, географія місць обробки таємної інформації й не в останню чергу розподіл повноважень між органами у сфері національної безпеки. В окремих країнах НАТО уповноважений орган з безпеки інформації входить до структури міністерств закордонних справ, оборони та юстиції, в інших країнах - його керівником є прем’єр-міністр або міністр внутрішніх справ.

Співробітництво між НАТО та країнами-партнерами, в тому числі з Україною, в рамках Ради євроатлантичного партнерства та Програми «Партнерство заради миру» також передбачає певні зобов’язання сторін щодо обміну інформацією та забезпечення її безпеки. Зокрема, перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи, на які покладається забезпечення безпеки інформації, мають бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити її захист відповідно до вимог сторони, котра її передає.

Приєднання країни до програми ПЗМ передбачає ратифікацію Угоди про безпеку між НАТО та країнами, які беруть участь у РЄАП та/або ПЗМ. Згідно з положеннями цієї Угоди сторони погоджуються консультуватися з політичних і безпекових питань, розширювати й інтенсифікувати політичне та військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах передбачає обмін учасників секретною інформацією або іншою інформацією з обмеженим доступом. Відповідальним органом при захисті інформації, якою обмінюються сторони при співробітництві в рамках РЄАП/ПЗМ, є NOS. Крім того, між НАТО та країною-партнером укладається окрема адміністративна угода щодо стандартів взаємного забезпечення безпеки інформації, якою обмінюються сторони, а також призначається офіцер зв’язку між NOS і національним органом з безпеки інформації. Всі дані, якими обмінюються сторони в рамках РЄАП/ПЗМ, є інформацією з обмеженим доступом і призначена тільки для урядового використання. На відміну від стандартів щодо захисту інформації, прийнятих в системі НАТО, в мінімальних стандартах з обробки і захисту таємної інформації, якою обмінюються сторони в рамках програм РЄАП/ПЗМ, немає рівня «цілком таємно», адже кількість такої інформації в системі НАТО вкрай обмежена, а додаткові вимоги із забезпечення безпеки інформації такого рівня таємності невиправдано ускладнили би процедуру взаємного обміну.

Незважаючи на те, що НАТО з часів створення постійно захищає свої інформаційні системи, на Празькому саміті 2002 року це питання було винесене до кола політичних. Беручи до уваги технічний прогрес, досягнутий після Празького саміту, лідери країн Альянсу на Ризькому саміті у 2006 році ще раз визнали необхідність забезпечення кібернетичної безпеки. Водночас, перед кібернападами на Естонію в 2007 році діяльність НАТО в галузі кіберзахисту зосереджувалася переважно на захисті комунікаційних систем, які належали Альянсу та використовувалися його членами. Кібернапади 2007 року змусили НАТО серйозніше замислитися над проблемами забезпечення безпеки кіберпростору, зокрема, сприймати загрози, що походять з Інтернет-простору, як стратегічно важливі. Надалі НАТО провела ретельну оцінку свого підходу до кіберзахисту, за результатами якої в жовтні 2007 року була підготовлена доповідь міністрам оборони країн-членів з рекомендаціями щодо конкретних завдань НАТО, а також нових заходів з удосконалення захисту від кібернападів. Офіційна політика НАТО у сфері кіберзахисту (NATO Cyber Defence Policy) була схвалена міністрами оборони держав-членів і представлена учасникам організації у квітні 2008 р. на саміті в Бухаресті. Її мета – «забезпечити можливості для надання підтримки країні-союзниці, на її вимогу, у протидії кібератаці».

Кількість та складність кібернападів швидко збільшувалася після нападів на Естонію в 2007 році, а вже влітку 2008 року війна РФ проти Грузії продемонструвала, що кібернапади стали основною складовою воєнних дій із застосуванням традиційної зброї. Тож у 2010 році на Лісабонському саміті НАТО було вирішено розробити нову політику організації з питань кіберзахисту, а також конкретний план дій, який набув чинності з червня 2011 року. В рамках їх реалізації НАТО використовує процеси оборонного планування з метою сприяння розвитку захисту союзників від кіберзлочинності, а також для оптимізації взаємодії, співробітництва та обміну інформацією. З питань протидії небезпекам, що виникають у кіберпросторі, НАТО тісно співпрацює за країнами ЄС та з ООН.

У Стратегічний концепції та Декларації Лісабонського саміту зазначається, що швидкий розвиток та постійне ускладнення кібернападів роблять захист інформаційно-комунікаційних систем країн-членів НАТО таким, від якого залежить майбутня безпека організації, а інформаційні атаки фігурують серед найнебезпечніших викликів і загроз безпеці та процвітанню держав-членів Альянсу. В ієрархії викликів, перелічених у вказаній концепції, загрози, які походять з інформаційного простору, розташовані одразу ж після поширення зброї масового знищення й тероризму. Така увага зумовлена, зокрема, феноменом секьюритизації, завдяки якому кібербезпека «еволюціонувала з технічної дисципліни у стратегічний концепт». Сьогодні НАТО забезпечує розвиток засобів запобігання, виявлення, реагування й відновлення після атак за допомогою створених Органу з управління кібернетичною безпекою, Спільного Центру передового досвіду з кіберзахисту і Сил реагування на комп’ютерні інциденти.

У заяві, оприлюдненій за результатами Варшавського саміту глав держав та урядів, які брали участь у засіданні Північноатлантичної ради у липні 2016 року, зазначається, що кібернапади становлять очевидний виклик безпеці Альянсу й можуть бути не менш згубними для сучасних суспільств, ніж напади із застосуванням звичайних видів зброї. Відтак, кіберзахист є частиною головного завдання НАТО – колективної оборони, а кіберпростір визнається сферою операцій, де НАТО має захищати себе так само ефективно, як робить це у повітрі, на землі та на морі. Це підвищить спроможність НАТО щодо захисту та проведення операцій у цих сферах, збереже свободу дій та рішень у будь-яких умовах та сприятиме забезпеченню НАТО ширшими можливостями стримування та оборони.

НАТО розвиває співробітництво з кіберзахисту відповідно до Вказівок щодо співпраці з кіберзахисту з партнерами та міжнародними організаціями 2008 року та Рамкового документу щодо співпраці з кіберзахисту між НАТО та країнами-партнерами 2009 року, визнаючи необхідність визначення спільних підходів до використання сучасних систем захисту інформації з урахуванням вимог інформаційної безпеки. Забезпечення безпеки інформації в разі створення спільних інформаційних та телекомунікаційних систем, де циркулює інформація з обмеженим доступом, відбувається шляхом розроблення пропозицій щодо захисту конфіденційного зв’язку з використанням обладнання НАТО, необхідного для створення відокремлених інформаційно-комунікаційних систем в органах влади, а також підвищення кваліфікації їх фахівців з питань захисту інформації у рамках ПЗМ.

Проблема забезпечення інформаційної безпеки НАТО, крім питань технічного забезпечення й стратегічного планування, має також і політичний вимір. Передусім це стосується можливості застосування статті 5 Вашингтонського договору до інформаційних атак. Основними протагоністами розширення дії принципу колективної відповідальності у сфері забезпечення інформаційної безпеки в системі НАТО виступають Естонія й, до певної міри, США. Зокрема, відзначається, що за своїм визначенням кібератаки не є «збройним нападом», тобто не підпадають під дію ст. 5, однак робить висновок, що Альянс «має об’єднатися у протидії атакам, що загрожують безпеці будь-кого із членів НАТО». Варто зазначити, що питання протидії загрозам інформаційній безпеці, зокрема й кібербезпеці, відносять до сфери «м’якої безпеки» (soft security), тоді як головним завданням НАТО традиційно вважається протидія конвенційним викликам безпеки – забезпечення «жорсткої безпеки» (hard security). Тому ще одним проблемним чинником, котрий проявляється на трансатлантичному рівні, є «поділ праці» між членами НАТО, внаслідок якого одні країни спеціалізуватися на темах «м’якої безпеки», а інші проводять «тверді» військові місії. Наслідком цього є розбіжність у підходах протидії: США, Франція, Велика Британія й Німеччина зіставляють інформаційну безпеку з військовою стратегією, натомість Естонія, котра не володіє потужним військовим потенціалом, наголошує на провідній ролі громадянського суспільства та приватного сектору.

Європейські держави, які умовно можна об’єднати під назвою «країни позаблокового статусу», належать до найрозвиненіших на континенті, в тому числі з точки зору темпів розвитку інформаційного суспільства, а також усвідомлення необхідності протидії кіберзагрозам, захист інформації та критичної інформаційної інфраструктури й інформаційно-психологічної безпеки громадян та забезпечення інформаційної безпеки в цілому як складової національної безпеки. Тож, обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку провідних європейських країн в інформаційній сфері, критично оцінюючи та адаптуючи до власних реалій їх позитивний досвід у сфері забезпечення інформаційної безпеки. У цьому контексті корисним та цікавим убачається досвід таких країн, як Австрія, Швейцарія, Фінляндія та Ірландія, адже вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства, створення розвиненої інфраструктури інформаційних технологій та забезпечення високого рівня доступу населення до них.

Із закінченням холодної війни біполярний світ став набагато складнішим, відтак втратила самостійну цінність концепція неприєднання, неучасті у військово-політичних союзах і т.п. Зокрема, позбулося свого безпосереднього змісту поняття нейтралітету, пов’язане з неучастю у війнах, тому такий статус ряду країн Європи залишається значною мірою даниною історичним традиціям. На сьогодні такі держави позначають як постнейтральні або позаблокові (буквально - неприєднані, non-aligned). Кожна із цих держав має власну історію нейтралітету, однак протягом останніх 20 років усі вони зіштовхнулися з проблемою доцільності збереження нейтрального статусу та з необхідністю запровадження тих або інших обмежень щодо нього. Аналогічна тенденція продовжує діяти й нині, оскільки міжнародні процеси й змістовне наповнення нових загроз, серед яких це і регіональні конфлікти, і міжнародний тероризм, і поширення зброї масового знищення, а також кіберзлочинність – вимагають від міжнародної спільноти узгоджених дій та масштабного співробітництва.

Особливе місце з-поміж країн позаблокового статусу посідає Швейцарія, котра не є ані членом НАТО, ані ЄС.

З 1992 року у Швейцарії діє Федеральний акт про захист даних, який втілює загальноєвропейські принципи захисту інформації, в тому числі так званих «чутливих» відомостей та, зокрема, персональних даних. У 2010 році Верховний суд Швейцарії надав додаткові гарантії конфіденційності персональних даних, підтримавши місцевого уповноваженого із захисту таких даних та ухваливши порядок, відповідно до якого збір інформації про IP-адреси користувачів файлообмінних мереж без їхньої згоди (в тому числі в контексті боротьби з порушеннями авторських прав) є незаконним.

У цілому забезпечення інформаційної безпеки електронних даних та інформаційних мереж здійснюється у Швейцарії відповідно до затвердженої у 2012 році Національної стратегії захисту від кіберризиків, метою якої визначено:

1. раннє виявлення кіберзагроз і небезпек;
2. підвищення стійкості критичної інфраструктури;
3. ефективне зниження кіберризиків, зокрема кіберзлочинності, кібершпигунства й кіберсаботажу.

На початку 2018 року Швейцарія розпочала розробку закону про інформаційну безпеку, позаяк визнано, що незаконне використання інформації та втручання в роботу інформаційних систем може серйозно вплинути на істотні інтереси держави та права її громадян. Ґрунтуючись на загальновизнаних міжнародних стандартах, закон про інформаційну безпеку має забезпечити єдину формально-правову основу для контролю й упровадження інформаційної безпеки у сфері компетенції Федерального уряду Швейцарії. Закон стосується насамперед федеральних органів державної влади – парламенту, федеральних судів, федеральної прокуратури, національного банку та ін. Приватні особи й бізнес підпадають під дію закону тільки у разі провадження інформаційно «чутливої» діяльності за дорученням федеральних органів. Федеральна рада прагне також поглибити співробітництво з кантонами, які мають бути представлені у відповідному координаційному органі та брати участь у стандартизації відповідних заходів. Серед іншого закон регулює питання управління ризиками, класифікує інформацію й установлює принципи безпеки у сфері використання інформаційно-технічних ресурсів. Передбачається, що закон про безпеку інформації матиме пріоритет над законодавством про свободу інформації.

Членство в ЄС накладає на країни обов’язки щодо дотримання стандартів цієї організації стосовно розвитку інформаційного суспільства та забезпечення інформаційної безпеки. Так, ще 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій», де, зокрема, визначено завдання забезпечення інформаційної безпеки:

1. захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;
2. забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;
3. забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій». 2001 року Європейська Комісія оприлюднила документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому окреслено сучасне бачення ЄС проблематики інформаційної безпеки та, зокрема, визначено такі засади європейської політики інформаційної безпеки:

1. підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
2. створення європейської системи попередження та інформування про нові загрози;
3. забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації;
4. правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;
5. зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо;
6. розвиток міжнародного співробітництва з питань інформаційної безпеки.

В Австрії, Фінляндії та Ірландії, як і в інших країнах ЄС, значна увага приділяється проблемам кібербезпеки, окресленим у Документі Європейської комісії «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», де остання визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, а саме:

• традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах);

• публікації незаконного контенту в електронних медіа;

• специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо).

Основними викликами безпеці інформаційних інфраструктур зазначених країн, як і ЄС в цілому, є:

• некоординовані внутрішньодержавні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;

• відсутність на європейському рівні партнерства між державним та приватним секторами;

• обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;

• відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Вагомим елементом інформаційної безпеки усіх без винятку країн ЄС є захист персональних даних, засади якого визначені директивою 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних». Обов’язкові для країн-членів ЄС нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 року, для Австрії, Фінляндії та Ірландії набувають чинності у 2018 році. У документі переглянуто цивільні права користувачів, відповідальність за схоронність даних, а також запроваджено деякі обмеження на переміщення даних між різними країнами. Важливим нововведенням убачається також запровадження більш суворого покарання за несвоєчасне повідомлення інформації про виток даних.

Одним із лідерів ЄС за показниками розвитку інформаційного суспільства справедливо вважають Фінляндію, адже в рейтингу країн Євросоюзу вона утримує першість за рівнем цифрової грамотності (понад 50% населення) й посідає друге місце за показником поширення мережі широкосмугового зв’язку (34% населення).

Головними державними інституціями, відповідальними за розробку та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій Фінляндії, Омбудсмен з питань захисту даних. До повноважень Міністерства транспорту та комунікацій належить розробка законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також розробка й реалізація національної політики у сфері інформаційної безпеки.

Стратегія національної безпеки Фінляндії, зазначаючи, що критична інфраструктура країни все більше залежить від інформаційних систем та мереж, передбачає мінімізацію відповідних ризиків важливим завданням забезпечення всеосяжної безпеки. Концепція всеосяжної безпеки, окрім традиційного сценарію протидії військовим загрозам, охоплює також інші проблеми на кшталт зміни клімату, дефіциту енергетичних та водних ресурсів, міграції, тероризму, торгівлі наркотиками, кібератак тощо.

Стратегія кібербезпеки Фінляндії, затверджена у 2013 році, наголошує на тому, що загрози, які виходять з кіберпростору, стають усе більш серйозними, адже кібератаки можуть використовуватися як інструмент політичного й економічного тиску, в тому числі в комплексі із традиційними військовими засобами. При цьому кіберпростір – це джерело величезного потенціалу та ресурсів, позаяк збільшує можливості розвитку бізнесу, працевлаштування та залучення іноземних інвесторів.

Що стосується Австрійської Республіки, то програми становлення інформаційного суспільства в цій країні втілюють політичну стратегію об’єднання Європи на базі новітніх технологій, інформаційно-комунікаційної інфраструктури та інтелектуального потенціалу регіону. На інформаційну політику Австрії значний вплив чинять міжнародні організації, що мають резиденції у Відні, складовою програм діяльності яких є розвиток інформаційного суспільства.

Стратегія кібербезпеки Австрії зазначає, що звичайні військові напади на країну в найближчій перспективі малоймовірні, натомість для Австрійської Республіки та ЄС в цілому все більшої актуальності набувають нові проблеми, ризики й загрози.

Напади з кіберпростору становлять безпосередню загрозу безпеці й належному функціонуванню державного апарату, економіки, науки й суспільства. Недержавні суб’єкти (приміром, злочинці, учасники організованих злочинних угруповань або терористи), а також державні суб’єкти (скажімо, секретні служби й військові) можуть зловживати можливостями кіберпростору у своїх власних цілях і перешкоджати його належному функціонуванню. Як загрози в кіберпросторі, так і його продуктивне використання практично не лімітовані. Тому головним пріоритетом Австрії є забезпечення безпеки й кібербезпеки на національному й міжнародному рівнях. Всеосяжна політика кібербезпеки означає, що зовнішня й внутрішня безпека, а також усі аспекти цивільної й військової безпеки тісно пов’язані та взаємозалежні. Забезпечення кібербезпеки виходить за межі компетенції традиційних органів безпеки й потребує залучення інструментів багатьох інших сфер безпекової політики.

Ірландію, де розташовані великі європейські офіси таких компаній, як Google і Facebook, часто називають європейською Силіконовою долиною, оскільки ця країна докладає багато зусиль для підготовки та працевлаштування ІТ-фахівців.

Національна стратегія кібербезпеки Ірландії на 2015-2017 роки передбачала, що уряд всіляко сприятиме стійкій та безпечній експлуатації комп’ютерних мереж і відповідної інфраструктури ірландськими громадянами й підприємствами. Розвиток і поширення інформаційно-комунікаційних технологій посприяв вагомому поліпшенню якості життя, появі інноваційних послуг та радикальним змінам в організації бізнесу. Відтак, держава, критична інфраструктура, юридичні особи й громадяни залежать від надійного функціонування інформаційно-комунікаційних технологій та Інтернету. Порушення роботи цих систем, яким би джерелом воно не було спричинене, створює безпосередню загрозу функціонуванню державного механізму й економіки, може відчутно вплинути на повсякденне життя мільйонів громадян. Тому на будь-яку загрозу безпеці кіберпростору потрібне своєчасне, надійне й послідовне реагування як на національному, так і на міжнародному рівні.

Вивчення практики європейських країн у побудові власних моделей правового забезпечення інформаційної безпеки, протидії кіберзагрозам, а також аналіз ряду міжнародних правових документів дає змогу нам резюмувати про відсутність єдиної моделі національної системи правового забезпечення інформаційної безпеки.

Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері. При цьому, з огляду на геополітичне положення України, її провідним орієнтиром мають стати передусім країни Центральної Європи, адже саме вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства шляхом створення розвиненої інфраструктури інформаційних технологій з унікально високим рівнем доступу населення до них, випереджаючи за цим показником інші країни світу.

Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, але й ЄС, який сьогодні об’єднує розвинуті країни, котрі відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах. 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій», де, зокрема, визначено завдання забезпечення інформаційної безпеки, а саме:

• захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;

• забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;

• забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій», де застосовано модель тріади CIA, яка передбачає такі основні характеристики інформаційної безпеки: 1) конфіденційність; 2) цілісність; 3) доступність.

У документі Європейської Комісії «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.), визначено базові засади Співтовариства до проблеми забезпечення інформаційної безпеки. Термінологічне сполучення «мережева та інформаційна безпека» трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, котрі становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, які надаються через ці мережі й системи. Згаданий документ визначає такі пріоритетні напрями європейської політики забезпечення інформаційної безпеки:

• підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;

• створення європейської системи попередження та інформування про нові загрози; • забезпечення технологічної підтримки;

• підтримка ринково орієнтованої стандартизації та сертифікації;

• правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;

• зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо;

• розвиток міжнародного співробітництва з питань інформаційної безпеки.

У всіх без винятку країнах ЄС питанням правового забезпечення інформаційної безпеки надається особлива увага. При цьому першочергового значення набувають питання протидії кіберзагрозам, які є складовими процесу забезпечення інформаційної безпеки. З 1999 року реалізуються програми «Безпечніший Інтернет», у рамках яких здійснюються заходи, спрямовані на боротьбу не лише зі шкідливим контентом, але й з небезпечною поведінкою в мережі.

Процес формування європейської глобальної системи правового забезпечення інформаційної безпеки має тривалий характер. Ще в 2007 році Європейська Комісія прийняла документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю». У даному документі, хоча й на рівні декларації, визначено кіберзлочини як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, котрі включають: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо)

Дещо пізніше, у 2009 році у Повідомленні Європейської Комісії «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» були визначені головні виклики та проблеми, які потребують першочергового реагування зі сторони країн ЄС, а також окреслило основні заходи щодо посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам. Відповідно до даного документу засадничими викликами безпеці інформаційної безпеки країн ЄС є:

• некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;

• відсутність на європейському рівні партнерства між державним та приватним секторами;

• обмежені можливості щодо раннього запобігання та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;

• відсутність міжнародного консенсусу стосовно пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Окрім зазначеного, важливим аспектом правового забезпечення інформаційної безпеки у рамках ЄС є питання інформаційної відкритості органів державної влади країн учасниць. У даному ракурсі слід також послатися і на рекомендації Ради Європи № R(81)19 «Про доступ до інформації, яка перебуває в розпорядженні державних органів». У даному документі відмічено, що для гарантування адекватної участі всіх у суспільному житті необхідно забезпечити, з урахуванням неминучих винятків та обмежень, доступ громадськості до інформації, що перебуває в розпорядженні державних органів усіх рівнів. Першочергово значення тут набувають питання захисту персональних даних.

З цього приводу, у резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18 грудня 2013 року визначено глобальну й відкриту природу Інтернету і швидкий розвиток у сфері інформаційних та комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі підтверджено, що «ті ж права, що люди мають в офлайн-режимі, мають також бути захищені онлайн, у тому числі право на приватність». Засади захисту персональних даних у правовій практиці країн ЄС можна звести до такого:

1. пріоритетність права особи розпоряджатися своїми персональними даними;
2. використання персональних даних без дозволу володільця тягне відповідальність згідно з законодавством;
3. для будь-кого, хто здійснює користування персональними даними фізичних осіб з їхнього дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (крім випадків, коли на це надано дозвіл).

Попри згадані документи ЄС про захист персональних даних, основним серед них слід вважати директиву 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних». У ньому декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та одночасно надаються гарантії захисту основних прав громадян, до яких належить і право на недоторканність особистих даних та їх захист від третіх осіб. Директива ЄС зобов’язує кожну державу-члена прийняти свої національні закони про захист приватних відомостей, які відповідали б рекомендаціями OECD 1980 року. З-поміж цих рекомендацій варто відзначити «Принцип гарантованої безпеки N11», який вимагає, аби «персональні дані були захищені розумними засобами безпеки від таких загроз, як утрата чи неавторизований доступ, руйнування, використання, модифікація або розголошення».

Обов’язкові для країн-членів ЄС нові правила захисту персональних даних, які ухвалено 14 квітня 2016 року, набувають чинності у 2018 році. Ці правила поширюватимуться не лише на європейські компанії, але й на суб’єктів інших країн, які пропонують товари й послуги в ЄС. У документі переглянуті цивільні права користувачів, відповідальність за схоронність даних, а також запроваджено деякі обмеження переміщення даних між країнами.

Слід констатувати, що країни ЄС сформували «в певному сенсі злагоджену систему захисту інформації», але водночас кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної безпеки.

Для нас, як країни яка заявила про свої наміри Євроінтеграції та членства в НАТО, цікави є досвід Румунії й Болгарії як членів НАТО та Європейського Союзу. Першочергово тому, що в цих країнах вже апробовані і діють стандарти ЄС та НАТО щодо інформаційної політики та правового забезпечення інформаційної безпеки. Зокрема, це стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору», офіційна політика НАТО у сфері кіберзахисту, стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського й уточнена за результатами Варшавського самітів [338], та ін. Як члени ЄС ці країни втілюють також у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені «Європейськими критеріями безпеки інформаційних технологій» (1991), «Єдиними критеріями безпеки інформаційних технологій» (1996), документами «Мережева та інформаційна безпека: європейський політичний підхід» (2001) і «На шляху до загальної політики у сфері боротьби з кіберзлочинністю» (2007) та ін.

Аналіз згаданих міжнародних документів дає змогу виокремити пріоритетні напрямами забезпечення інформаційної безпеки у цих країнах:

• підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;

• створення європейської системи попередження та інформування про нові загрози;

• забезпечення технологічної підтримки;

• підтримка ринково орієнтованої стандартизації та сертифікації;

• правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;

• зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо;

• розвиток міжнародного співробітництва з питань інформаційної безпеки.

Попри зазначені пріоритети важливо значення на рівні законодавства надається захисту персональних даних. У Директиві 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та надаються гарантії захисту основних прав громадян, до яких належить право на недоторканність особистих даних та їх захист від третіх осіб.

РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА

2.1 Визначення поняття безпеки

2.1.1 Визначення поняття безпеки в законодавстві України

|  |  |  |  |
| --- | --- | --- | --- |
| № | Визначення | Нормативно-правовий акт | Чинність НПА |
| 1. | Безпека - відсутність неприпустимого ризику, пов'язаного з можливістю завдання будь-якої шкоди для життя, здоров'я та майна громадян, а також для навколишнього природного середовища. | Наказ Державного комітету будівництва, архітектури та житлової політики України, Державного комітету України по нагляду за охороною праці «Про заходи щодо виконання постанови Кабінету Міністрів України від 05.05.97 N 409 "Про забезпечення надійності й безпечної експлуатації будівель, споруд та інженерних мереж"» | втратив чинність |
| 2. | Безпека - комплекс заходів, а також людські і матеріальні ресурси, які призначені для захисту цивільної авіації від актів незаконного втручання та інших протиправних посягань. | Наказ Державного департаменту авіаційного транспорту України «Про затвердження Правил супроводження в контрольованих зонах авіапідприємств матеріальних цінностей і пасажирів» | чинний |
| 3. | безпека - відсутність неприпустимого ризику, пов'язаного з травмуванням або загибеллю людей, заподіянням збитків навколишньому середовищу | Наказ Міністерства транспорту України «Про затвердження Правил супроводження в контрольованих зонах авіапідприємств матеріальних цінностей і пасажирів» | втратив чинність |
| 4. | Безпека - властивість об'єкта забезпечувати відсутність ризику завдання шкоди здоров'ю людей, майну та навколишньому середовищу. | Наказ Міністерства промислової політики України «Про затвердження Положення про технічне обслуговування устаткування підприємств гірничо-металургійного комплексу» | чинний |
| 5. | безпека - відсутність неприпустимого ризику, пов'язаного з травмуванням або загибеллю людей, заподіянням збитків майну та довкіллю | Наказ Міністерства транспорту та зв’язку України «Про затвердження Положення про систему управління безпекою руху поїздів у Державній адміністрації залізничного транспорту України» | втратив чинність |
| 6. | безпека (safety) - стан, при якому ризик шкоди чи ушкодження обмежений до прийнятного рівня | Наказ Міністерства транспорту та зв’язку України «Про затвердження Правил сертифікації суб'єктів, що надають послуги з аеронавігаційного обслуговування. | чинний |
| 7. | "Безпека" – комплекс заходів, а також людські та матеріальні ресурси, які призначені для захисту від актів незаконного втручання й інших протиправних посягань стосовно цивільної авіації | Угода між Урядом України і Урядом Азербайджанської Республіки про співробітництво в галузі авіаційної безпеки | чинний |
| 8. | безпека - відсутність загрози життю, здоров'ю людей, майну, тваринам, рослинам і довкіллю, що перевищує граничний ризик; | Наказ Міністерства інфраструктури України «Про затвердження Положення про систему управління безпекою руху поїздів у Державній адміністрації залізничного транспорту України» | чинний |
| 9. | безпека - відсутність недопустимого ризику, пов’язаного з можливістю спричинення шкоди та/або нанесення збитку | Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг «Про затвердження Кодексу систем розподілу» | чинний |
| 10. | безпека - відсутність ризику, пов’язаного з можливістю спричинення шкоди та/або нанесення збитку | Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг «Про затвердження Кодексу системи передачі» | чинний |
| 11. | безпека - запобігання використанню вибухових матеріалів, що суперечить закону та загрожує громадському порядку | Постанова Кабінету Міністрів України «Про затвердження Технічного регламенту вибухових матеріалів промислового призначення» | чинний |

Виходячи від логіко-детермінантного підходу до розуміння поняття «Безпека», Заплатинський В. М. наводить таке визначення: безпека — це такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень.

2.1.2 Види безпеки

|  |  |  |
| --- | --- | --- |
| Безпека людини | такий стан людини, коли дія зовнішніх та внутрішніх факторів не призводить до смерті, погіршення функціонування та розвитку організму, свідомості, психіки та людини в цілому і не перешкоджає досягненню певних бажаних, для людини, цілей. | |
| Національна безпека | захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам. Складовими національної безпеки є: | |
| а) | Державна безпека |
| б) | Політична безпека |
| в) | Економічна безпека |
| г) | Воєнна безпека |
| ґ) | Технологічна безпека |
| д) | Екологічна безпека |
| е) | Гуманітарна безпека |
| є) | Демографічна безпека |
| ж) | Інформаційна безпека |
| з) | Банківська безпека |
| и) | Інвестиційна безпека |
| і) | Продовольча безпека |
| ї) | Енергетична безпека та інші |
| Безпека життєдіяльності | спрямована захисту здоров'я та життя людини і середовища її проживання від небезпек. Складовими безпеки життєдіяльності є: | |
| а) | Безпека праці |
| б) | Безпека військової служби |
| в) | Громадська безпека тощо |
| Безпека конкретних видів діяльності | виробнича безпека: | |
| а) | Ядерна безпека |
| б) | Гірнича безпека |
| в) | Віброакустична безпека, |
| г) | Безпека харчових продуктів |
| Безпека споруд і об'єктів | властивість споруди не створювати загрозу для життя, здоров'я та інтересів людини: | |
| а) | Техногенна безпека |
| б) | Пожежна безпека |
| в) | Радіаційна безпека тощо |
| безпека особиста | | |
| безпека побутова | | |

2.2 Визначення поняття інформації

2.2.1 Визначення поняття інформації в законодавстві України

|  |  |  |  |
| --- | --- | --- | --- |
| № | Визначення | Нормативно-правовий акт | Чинність НПА |
| 1. | Інформація - сукупність відомостей, знань і повідомлень про об`єкти, явища і процеси. | Постанова Кабінету Міністрів України «Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи» | втратив чинність |
| 2. | інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді | Закон України «Про інформацію» | чинний |
| 3. | інформація - відомості в будь-якій формі та вигляді, на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відеофільми, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості | Закон України «Про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності» | втратив чинність |
| 4. | інформація - відомості в будь-якій формі та вигляді, на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відеофільми, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їхніх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості | Постанова Національної комісії регулювання електроенергетики України «Про затвердження Умов та Правил здійснення підприємницької діяльності (ліцензійних умов) з транспортування нафти магістральними трубопроводами» | втратив чинність |
| 5. | інформація - відомості в будь-якій формі та вигляді, на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відеофільми, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості | Закон України «Про захист економічної конкуренції» | чинний |
| 6. | інформація - відомості в будь-яких формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості | Положення Антимонопольного комітету України «Про затвердження Положення про порядок подання заяв до Антимонопольного комітету України про попереднє отримання дозволу на концентрацію суб'єктів господарювання (Положення про концентрацію)» | чинний |
| 7. | Інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. | Цивільний кодекс України | чинний |
| 8. | інформація - відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб; | Закон України «Про телекомунікації» | чинний |
| 9. | информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их регистрации и представления | Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых Государств в сфере информатизации | чинний |
| 10. | "інформація" означає будь-які дані незалежно від того, чи були вони піддані обробці й аналізу, а також документи, звіти й інші повідомлення в будь-якій формі, зокрема електронній, або їхні засвідчені копії | Угода між Україною та Королівством Нідерландів про взаємну адміністративну допомогу в митних справах | чинний |
| 11. | "Інформація" — будь-яка інформація, наведена у Статті IV, що стосується операції "Чорноморська гармонія" (далі — ОЧГ), і якою Сторони обмінюються у відповідності до національного законодавства, Угоди і цього Протоколу у письмовій, усній, аудіовізуальній або електронній формі (фільми, слайди, фотографії, касети, дискети тощо) | Протокол між Міністерством оборони України та Генеральним штабом Збройних Сил Турецької Республіки про співробітництво з питань обміну інформацією у рамках операції "Чорноморська гармонія" | чинний |
| 12. | "інформація" означає будь-які дані, незалежно від того, чи проводились їхня обробка та аналіз, а також документи, звіти й інші повідомлення в будь-якій формі, зокрема електронній, або засвідчені чи оригінальні примірники цих матеріалів | Міжнародна конвенція про адміністративну взаємодопомогу у сфері митних відносин | чинний |
| 13. | "Інформація" означає звіти, записи, документи та документацію в електронній або паперовій формі, а також їх копії | Угода між Кабінетом Міністрів України та Урядом Соціалістичної Республіки В'єтнам про співробітництво та взаємну адміністративну допомогу в митних справах | чинний |
| 14. | Інформація - інформація, що підлягає розміщенню у Загальнодоступній інформаційній базі даних про ринок цінних паперів відповідно до вимог законодавства | Рішення Національної комісії з цінних паперів та фондового ринку «Про затвердження Положення щодо порядку взаємодії осіб, що зобов'язані розкривати інформацію на фондовому ринку, з особою, уповноваженою Національною комісіє ю з цінних паперів та фондового ринку на розміщення інформації в загальнодоступній інформаційній базі даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів» | чинний |
| 15. | інформація - будь-які неперіодичні відомості та/або дані, у тому числі такі, що містять фінансово-економічні показники діяльності операторів, провайдерів телекомунікацій, необхідні НКРЗІ для виконання своїх повноважень | Рішення Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації «Про затвердження Порядку надання операторами, провайдерами телекомунікацій звітності та інформації і визнання такими, що втратили чинність, рішень НКРЗ від 04.11.2008 № 1189 та від 25.12.2008 № 1283» | чинний |
| 16. | інформація - відомості (дані) в електронному вигляді | Наказ Міністерства внутрішніх справ України «Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС» | втратив чинність |
| 17. | «інформація» - персональні та інші дані, передбачені цією Угодою, щодо осіб і транспортних засобів, на яких особи перетинають українсько-молдовський державний кордон та яка перебуває у відповідних базах даних компетентних органів держав Сторін (далі - компетентні органи) | Угода між Кабінетом Міністрів України та Урядом Республіки Молдова про організацію обміну інформацією про осіб, транспортні засоби, на яких особи перетинають українсько-молдовський державний кордон | чинний |
| 18. | "інформація" - персональні та інші дані, що передбачені цим Протоколом, якими Сторони обмінюються у процесі функціонування контактних пунктів | Протокол між Адміністрацією Державної прикордонної служби України і Департаментом Прикордонної поліції Міністерства внутрішніх справ Республіки Молдова про контактні пункти на українсько-молдовському державному кордоні | чинний |
| 19. | Термін "інформація" означає дані в будь-якій формі, незалежно від того, чи були вони піддані обробці або аналізу, а також документи, звіти й інші повідомлення в будь-якій формі, включаючи їх електронні, завірені або засвідчені копії | Угода між Урядом України та Урядом Сполучених Штатів Америки про взаємну допомогу між їх митними адміністраціями | чинний |

2.2.2 Міжнародні стандарти, в яких наведено визначення інформації

|  |  |
| --- | --- |
| ISO/IEC 10746-2:1996 | Інформація – знання про предмети, факти, ідеї і т.д., якими можуть обмінюватися люди в рамках конкретного контексту |
| ISO/IEC 2382:2015 | Інформація – знання щодо фактів, подій, речей, ідей і понять, які в певному контексті мають конкретний зміст |
| ISO/IEC/IEEE 24765:2010 | Інформація вважається нематеріальною, а то, що міститься в структурі об'єктів, називається даними |

Складність однозначного визначення судження інформація, пов'язана з тим, що цей термін використовується в багатьох областях людської діяльності, тобто є багатогранним. Спеціалістів із теорії зв'язку цікавить насамперед передача інформації від джерела до отримувача без спотворень, філософа – розуміння змісту, фахівця з комп'ютерної науки – процеси запису, зчитування, зберігання й обробки, диктора на радіо – доведення повідомлення до відома широкого кола слухачів.

Існують переважно несумісні між собою визначення судження «інформація». Але практично всі погляди на сутність інформації групуються навколо двох концепцій – атрибутивної та функціональної. Атрибутивна концепція інформації наголошує на тому, що інформація є атрибутом (невід'ємною властивістю) об'єктів. Функціонально-кібернетична концепція вважає, що головним у інформації є та функція, яку вона виконує. Особливо цікавою є функція, яку відіграє інформація, закладена, наприклад, у ДНК в розвитку біологічних організмів та інших систем, в яких можлива самоорганізація.

2.2.3 Класифікація інформації

|  |  |  |  |
| --- | --- | --- | --- |
| Інформацію можна розділити на види за різними критеріями: | | | |
| 1. | За способом сприйняття : | | |
| Візуальна | прийнята органами зору | |
| Звукова | сприйнята органами слуху | |
| Тактильна | сприйнята тактильними рецепторами | |
| Нюхова | сприйнята нюховими рецепторами | |
| Смакова | сприйнята смаковими рецепторами | |
| 2. | За формою подання : | | |
| Текстова | що передається у вигляді символів, призначених позначати лексеми мови | |
| Числова | у вигляді цифр і знаків (символів), що позначають математичні дії | |
| Графічна | у вигляді зображень, предметів, графіків | |
| Звукова | усна або у вигляді запису і передачі лексем мови аудіальним шляхом | |
| Відеоінформація | | передана у вигляді відеозапису |
| 3. | За призначенням : | | |
| Масова | містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму | |
| Спеціальна | містить специфічний набір понять, при використанні відбувається передача відомостей, які можуть бути не зрозумілі основній масі соціуму | |
| Секретна | передана вузькому колу осіб і за закритими (захищеним) каналам | |
| Особиста (приватна) | набір відомостей про яку-небудь особистості, що визначає соціальний стан і типи соціальних взаємодій всередині популяції | |
| 4. | За значенням: | | |
| Актуальна | інформація, цінна в даний момент часу | |
| Достовірна | інформація, отримана без спотворень з надійних джерел | |
| Зрозуміла | інформація, виражена мовою, зрозумілою того, кому вона призначена | |
| Повна | інформація, достатня для прийняття правильного рішення або розуміння | |
| Цінна | корисність інформації визначається суб'єктом, який отримав інформацію в залежності від обсягу можливостей її використання | |
| 5. | За істинності: | | |
| Справжня | | |
| Хибна | | |

2.3 Визначення поняття інформаційної безпеки

2.3.1 Визначення поняття інформаційної безпеки в українському законодавстві

|  |  |  |  |
| --- | --- | --- | --- |
| № | Визначення | Нормативно-правовий акт | Чинність НПА |
| 1. | информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства | Угода про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав - учасниць СНД | чинний |
| 2. | інформаційна безпека - комплекс організаційних заходів банку, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях банку та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності банку або його клієнтів | Постанова Правління Національного банку України «Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах» | чинний |

2.3.2 Визначення поняття інформаційної безпеки в ГСТУ СУІБ 2.0/ISO/IEC 27002:2010

|  |  |  |
| --- | --- | --- |
| № | Вступ | |
| 0.1 | Що таке інформаційна безпека? | |
| Інформація є активом, який подібно іншим важливим діловим активам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов’язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов’язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та вразливостей (див. також OECD Guidelines for the Security of Information Systems and Networks). | |
| НАЦІОНАЛЬНЕ ПОЯСНЕННЯ.  Рекомендації Організації економічного співробітництва та розвитку щодо безпеки інформаційних систем та мереж | |
| Інформація може існувати у багатьох формах. Вона може бути надрукована або написана на папері, збережена в електронному вигляді, переслана поштою або з використанням електронних засобів, показана на плівці або сповіщена у бесіді. Незалежно від набутого виду інформації або засобів, за допомогою яких вона поширюється або зберігається, вона повинна завжди бути відповідно захищена. | |
| Інформаційна безпека - це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес ризику і максимізації рентабельності інвестицій і бізнес можливостей. | |
| Інформаційна безпека досягається впровадженням відповідного набору контролів, який охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці контролі необхідно розробити, впровадити, моніторити, переглядати та, за необхідності, вдосконалювати для гарантування того, що певні безпека та бізнес-цілі організації будуть досягнуті. Це треба виконувати узгоджено з іншими процесами управління бізнесом. | |
| Національна примітка. | |
| Питання щодо інформаційної безпеки визначаються Законами України: | |
| а) | Про інформацію |
| б) | Про захист інформації в інформаційно-телекомунікаційних системах |
| в) | Про електронний документ і електронний документообіг |
| г) | Про електронний цифровий підпис |
| Питання інформаційної безпеки для банківської діяльності визначаються Законами України: | |
| а) | Про Національний банк України |
| б) | Про банки і банківську діяльність |
| в) | Про платіжні системи та переказ коштів в Україні |
| та нормативними документами Національного банку України | |

2.3.3 Інформаційна безпека – напрям реалізації в Розпорядженні Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2013 р. № 386-р

Інформаційна безпека

Забезпечення інформаційної безпеки у процесі використання інформаційно-комунікаційних технологій є однією з найважливіших умов успішного розвитку інформаційного суспільства. Пріоритетами діяльності в галузі забезпечення інформаційної безпеки є:

сприяння виробництву конкурентоспроможного національного інформаційного продукту;

сприяння вітчизняному виробництву засобів захисту інформації, створенню захищених інформаційно-телекомунікаційних систем, запровадження сучасних захищених інформаційних технологій в інтересах державного управління;

створення ефективної системи виявлення та запобігання загрозам державних електронних інформаційних ресурсів, у тому числі щодо протидії розповсюдженню комп’ютерних вірусів, програмних і апаратних закладок, а також витоку інформації технічними каналами та за рахунок несанкціонованих дій;

забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів України, які створюють умови для розвитку особи, стійкого функціонування суспільства і держави, захисту персональних даних та інформації, що перебуває у володінні фізичних, юридичних осіб та держави, від зовнішніх і внутрішніх інформаційних загроз, зокрема шляхом протидії комп’ютерним злочинам;

забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та органів місцевого самоврядування, інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, задовольняють потреби оборони та безпеки держави, кредитно-банківських та інших сфер національної економіки, систем управління об’єктами критичної інфраструктури;

удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема кібернетичної безпеки національної критичної інфраструктури;

впровадження захищеного механізму ідентифікації учасників електронної взаємодії.

2.4 Визначення поняття міжнародно-правових стандартів

2.4.1 Особливості поняття міжнародно-правового регулювання

Під міжнародно-правовими стандартами розуміються міжнародно-правові норми, що регулюють та регламентують принципи, особливості контролю певної сфери.

|  |  |  |
| --- | --- | --- |
| 1. | Норма міжнародного права — це створене за згодою держав та інших суб’єктів міжнародного права формально визначене правило поведінки, що регулює міжнародні відносини шляхом запровадження прав та обов’язків для суб’єктів і забезпечується юридичним механізмом охорони. | |
| 2 | До характерних рис, що вирізняють міжнародно-правові норми від інших суспільних норм поведінки (будь то моральні, політичні, релігійні чи інші норми) належать: | |
| 1) | об’єкт регулювання |
| 2) | метод регулювання |
| 3) | координаційний характер цих норм |
| 4) | обов’язковість тільки для сторін, які добровільно їх визнали |
| 5) | форма існування (міжнародні договір, звичай, акти міжнародних міжурядових організацій тощо) |
| 6) | забезпечення реалізації здійснюється суб’єктами міжнародного права |
| 7) | структурна особливість |
| 3. | Об’єктом регулювання є особливий різновид суспільних відносин, а саме міжнародні правовідносини. Ці відносини визначають і специфіку методу міжнародно-правового регулювання. | |
| 4. | Норми міжнародного права створюються на засадах добровільних угод між його суб’єктами. У результаті компромісів, поступок та узгоджень держави приходять до взаємно погодженого рішення про певні правила взаємовідносин. Закріплені в загальновизнаних юридичних формах, джерелах міжнародного права (міжнародних договорах та звичаях, певних актах міжнародних організацій), вони визнаються нормами міжнародного права, які мають «погоджувальний», «координаційний» характер. Це відрізняє їх від норм національного права, які мають «субординаційний» характер і виражають не узгоджені між окремими суб’єктами права правила поведінки, а встановлені державою через законодавство обов’язкові для них норми, виконання яких гарантується органами державного примусу. | |
| Також норми міжнародного права відрізняються від національних тим, що більшість з них не має загальнообов’язкового характеру. Група держав або навіть більшість держав не можуть створювати норми для інших держав. Кожна договірна або звичаєва норма втілюється в об’єктивне право тільки для держав, які беруть участь у них або висловили з ними явну чи мовчазну згоду. | |
| 5. | Структура норм міжнародного права | |
| Специфіка міжнародно-правових норм полягає в особливостях їхньої внутрішньої структури, їх конструкції. Як відомо, більшість національно-правових норм складається з трьох частин: гіпотези, тобто вказівки на ті умови, за яких застосовується відповідне правило поведінки; диспозиції, тобто самого правила поведінки; і санкції, тобто вказівки на ті заходи державного примусу, що застосовуються в разі порушення диспозиції. Норми міжнародного права найчастіше містять лише диспозицію (правило належної поведінки), рідше — гіпотезу та диспозицію, а санкція, тобто межі відповідальності за порушення диспозиції, як структурний елемент норми відсутня. | |
| Санкції в доктрині міжнародного права називаються ще контрзаходами. Вони визначаються системою у цілому. Існує навіть самостійний інститут міжнародно-правових санкцій, який регулює застосування їх потерпілими державами індивідуально або колективно стосовно до держав-правопорушників. Санкції можуть визначатися також в конкретних договорах, добровільно укладених між зацікавленими сторонами. | |

2.4.2 Класифікація міжнародно-правових норм

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Ускладнення правових функцій визначає багатоманітність нормативного інструментарію. З’являються нові види норм, удосконалюється їх взаємодія у системі. Про поглиблення системного характеру міжнародного права свідчить, зокрема, зростання кількості норм, які здатні здійснювати регулюючий вплив лише у сукупності з іншими нормами | | |
| 2. | Беручи за основу лише найбільш важливі критерії, можна запропонувати наступну класифікацію міжнародно-правових норм: | | |
| 1) | за сферою дії: | |
| а) | універсальні |
| б) | регіональні |
| в) | локальні |
| г) | партикулярні |
| 2) | за змістом і місцем у системі: | |
| а) | цілі |
| б) | принципи |
| в) | норми |
| 3) | за юридичною силою: | |
| а) | імперативні |
| б) | диспозитивні |
| в) | рекомендаційні |
| 4) | за функціями у системі: | |
| а) | матеріальні |
| б) | процесуальні |
| 5) | за способом створення та формою існування, тобто за джерелом: | |
| а) | загальні |
| б) | договірні |
| в) | норми рішень міжнародних організацій |
| 6) | за характером нормативних приписів: | |
| а) | зобов’язальні |
| б) | заборонні |
| в) | уповноважувальні |
| г) | відсильні |
| 7) | за терміном дії: | |
| а) | строкові |
| б) | безстрокові |
| Без універсального міжнародного права глобальна система міжнародних відносин функціонувати не може. Головними відмінними ознаками універсальних норм є всезагальна обов’язкова сила, створення та відміна їх міжнародною спільнотою у цілому. Основною формою існування служить звичай. Універсальні норми утворюють загальне міжнародне право | | |
| 3. | Існують норми, які приймаються обмеженою кількістю держав, але мають всезагальне значення. Такі норми встановлюють міжнародний режим (наприклад, для Антарктики, для космічного простору тощо). Норми створюються найбільш зацікавленими державами і поступово знаходять визнання з боку інших держав. Виходить, що і у даному випадку норми приймаються спільнотою у цілому. | | |
| Універсальні норми — це норми, що регулюють відносини, об’єкт яких становить загальний інтерес світового співтовариства, і спрямовані на визнання їх переважною більшістю або всіма державами. | | |
| 4. | Регіональні норми історично передували універсальним. Останні створювалися на базі перших, використовуючи їх досвід. Цей процес продовжується й досі. Разом з тим універсальне міжнародне право сприяє прогресу регіональних систем, передаючи їм досвід як більш розвинутих регіональних систем, так і універсальної системи. | | |
| Статут ООН містить главу «Регіональні угоди», яка присвячена специфічному регіоналізму — військово-політичному. У ст. 52 цього статут зазначено, що такі угоди чи їх органи та їх діяльність повинні бути сумісними з цілями та принципами ООН. | | |
| Регіональні норми — це норми, що регулюють будь-які міждержавні відносини, об’єкт яких має регіональний інтерес і які визнаються всіма або більшістю держав відповідного регіону. | | |
| 5. | Локальні норми регулюють відносини між державами певної місцевості, здебільшого між сусідніми, стосовно об’єктів, які знаходяться в даній місцевості. Їх основним джерелом є договори. Але існують і звичайні норми такого. роду. Міжнародний Суд ООН не один раз посилався на регіональні, локальні звичаї. | | |
| Локальні норми за кількістю значно перевищують універсальні. Вони виконують важливі функції по відношенню до останніх, а саме слугують засобом їх конкретизації стосовно певних випадків, сприяють їх реалізації у цих випадках та регулюють відносини, що не охоплюються загальним міжнародним правом. Такі норми містяться, наприклад, у Конвенції про захист морського середовища в районі Балтійського моря від 22 березня 1974 року. | | |
| 6. | Партикулярні норми — це найпоширеніший вид норм міжнародного права. Вони регулюють міждержавні відносини між будь-якими державами, з приводу будь-яких об’єктів, незалежно від географічного розташування держав і географічних особливостей об’єктів правового регулювання. Такі норми можуть бути багатосторонніми, але частіше за все регулюють певні двосторонні відносини взаємодіючих суб’єктів, розташованих у різних географічних регіонах. Такі норми втілені, наприклад, у Консульській Конвенції між Україною і Соціалістичною Республікою В’єтнам від 8 червня 1994 року. | | |
|  | Виділяють організаційні норми, які регулюють діяльність міжнародних органів та організацій. Науково-технічна революція обумовили швидкий розвиток технічних зв’язків. Потреба в їх регулюванні спричинила розповсюдження технічних норм. До них відносяться норми міжнародного права, які надають юридичну силу вимогам, що витікають із законів природи, науки і техніки. Технічні норми регулюють не функціонування технічних систем, а співробітництво держав, зобов’язуючи їх забезпечити дотримуватися встановлених правил тими, хто експлуатує ці системи. За своїм змістом норми є технічними, але за механізмом дії — міжнародно-правовими. | | |

Процес створення та особливості імперативних норм (jus cogens)

|  |  |
| --- | --- |
| Серед усіх норм міжнародного права особливе місце посідають імперативні норми. Уперше вони одержали офіційне, універсальне та юридичне закріплення в міжнародному договорі універсального характеру — Віденській конвенції про право міжнародних договорів 1969 року, потім були відображені у Віденській конвенції про право договорів між державами та міжнародними організаціями або між міжнародними організаціями 1986 року. Хоча ще у минулому існувало імперативне регулювання, яке визначало порядок створення норм — лише угодами. Імперативний був принцип pacta sunt servanda (договори мають виконуватися), без якого нема міжнародного права. Імперативними були заборони піратства та работоргівлі, а також деякі правила ведення війни. Новизна полягає у тому, що тепер імперативні норми утворюють цілий комплекс, що визначає характер міжнародного права, його цілі та принципи, основний зміст. Окрім того, імперативні норми отримали офіційне визнання. | |
| Відповідно до ст. 53 зазначених Конвенцій імперативна норма загального міжнародного права є нормою, що приймається і визнається міжнародним співтовариством держав у цілому як норма, відхилення від якої неприпустиме і яку може бути змінено лише наступною нормою загального міжнародного права, що має такий самий характер. У статті ставиться знак рівності між дефініціями «імперативні норми» та jus cogens. | |
| У цьому визначенні можна виділити чотири істотних аспекти. | |
| 1) | відноситься до юридичної природи норм jus cogens, полягає у тому, що ця норма є результатом узгодження воль держав та міжнародних міжурядових організацій та в її основі полягає угода між ними. Вона може бути явно висловлена через міжнародний договір, або мовчазна — через міжнародно-правовий звичай. При створені диспозитивних норм суб’єкти міжнародного права узгоджують свої волі спочатку відносно змісту правил поведінки, а після відносно визнання цього правила обов’язковим у міжнародному спілкуванні. У випадку створення імперативної норми загального міжнародного права, що мають характер jus cogens, необхідна додаткове волевиявлення держав та міжнародних міжурядових організацій на цей рахунок, тобто досягнення угоди про так би мовити більшу обов’язковість такої норми. Ця угода буває, як правило, мовчазною. |
| 2) | Другий аспект полягає в тому, що ця норма є загальновизнаною. |
| 3) | найбільш істотний аспект у тому, що ця норма має найвищу юридичну силу. Відхилення від імперативної норми неприпустиме як у двосторонніх, так і в багатосторонніх договорах. Будь-який договір є несуттєвим, якщо в момент укладання він суперечив імперативній нормі загального міжнародного права. |
| 4) | Четвертий аспект, тісно пов’язаний з першим, стосується можливості зміни норм jus cogens. Локальна угода держав відносно зміни її змісту є недійсною. Вона може бути змінена тільки наступною нормою загального міжнародного права, яка має імперативний характер. |
| Особливістю імперативних норм є те, що вони покликані регулювати найважливіші загальні відносини міжнародного співтовариства у цілому, і їх порушення завдає шкоди завдає шкоди усьому міжнародному співтовариству, а не окремим державам. Ще однією особливістю є те, що імперативні норми дійсно мають бути визнані всіма суб’єктами міжнародного права. Вони також служать критерієм оцінювання юридичної дійсності інших норм міжнародного права. | |
| Імперативні норми не кодифіковані, але імперативний характер носять усі основні принципи сучасного міжнародного права, які є головним критерієм правомірності усіх міжнародно-правових норм. Найширше визнання одержали такі види імперативних норм, як: | |
| 1) | рівноправність і самовизначення народів |
| 2) | незастосування сили та мирне вирішення спорів |
| 3) | загальнодемократичні стандарти елементарної гуманності та основних прав людини |
| 4) | неприпустимість привласнення «нічийних» земельних, морських, повітряних і космічних просторів, які мають життєво важливе значення для всієї міжнародної спільноти |
| Наявність у міжнародному праві імперативних норм не стримує процесу створення нових прогресивних норм, що спрямовані на більш ефективне забезпечення міжнародного миру та безпеки, на подальший розвиток довгочасного взаємовигідного співробітництва держав та міжнародних міжурядових організацій, а також інших суб’єктів міжнародного права. | |
| У літературі іноді підіймається питання щодо поширення норм jus cogens, прийнятих у межах ООН щодо держав, які не входять у цю міжнародну міжурядову організацію. Це пов’язано із тим, що визначив головні устої сучасного міжнародного правопорядку, його основні принципи, Статут ООН встановив: «Організація забезпечує, щоб держави, які не є її членами, діяли у відповідності з цими принципами, оскільки це може виявитися необхідним для підтримання міжнародного миру та безпеки» (п. 6 ст. 2 Статуту ООН). У зв’язку із щодо зобов’язань третіх держав, указується на буцімто об’єктивний характер закріплених норм, що вони відображають норми природного права, а тому є обов’язковими для усіх без винятку держав. | |
| Це питання слід визнати неактуальним, зважаючи на сучасну історію ООН. У період з березня 1992 по квітень 1993 року до ООН увійшли майже всі колишні союзні республіки Радянського союзу, Югославії та Чехословаччини. Прибалтійські держави ввійшли до організації ще 17 вересня 1991 року, Союзна республіка Югославія у складі Сербії та Чорногорії 1 листопада 2000 року (після проголошення у червні 2006 року незалежності Чорногорії, остання увійшла до складу ООН як окрема держава, а Сербія продовжила членство). У вересні 2002 року після входження до складу Організації Об’єднаних Націй до того завжди нейтральної Швейцарії та Східного Тимору, що врешті проголосив незалежність, завершився процес об’єднання під егідою організації усіх без винятку держав світу! Після цього ООН отримала принципово нове право, що в цілому не характерно для міжнародних організацій — визнання новостворених держав. Так, воно було реалізовано 28 червня 2006 року, коли Чорногорію було прийнято до лав міжнародного співтовариства. І тепер не існує держав, які не входять до складу ООН, а отже і територій, що не підпадають під її юрисдикцію. Тому норми jus cogens, прийняті у межах ООН, розповсюджуються і на території невизнаних держав, оскільки формально-юридично вони є територіями держав-членів ООН. | |

Диспозитивні та рекомендаційні норми

|  |  |
| --- | --- |
| 1. | Імперативні норми складають незначну кількість норм міжнародного права, тоді як їх основна частина — це диспозитивні норми. Це тому, що міжнародне право має координаційний характер, і держави як суверенні суб’єкти міжнародного права основний обсяг різноманітних міждержавних відносин урегульовують не за допомогою загальнообов’язкових норм. |
| 2. | Диспозитивні норми — це норми, що допускають відступ від них за угодою у взаємовідносинах сторін. Але це не повинно стосуватися прав та законних інтересів третіх держав. Більшість універсальних та локальних норм складають норми диспозитивні. У цьому знаходить своє вираження високий рівень індивідуалізації міжнародно-правового регулювання. Диспозитивні норми мають бути відповідними до імперативних норм, у протилежному випадку вони є недійсними. |
| Диспозитивні норми мають повну юридичну силу. Якщо суб’єкти не домовилися про інакше, то вони зобов’язані виконувати диспозитивну норму, а у випадку її порушення несуть відповідальність. Диспозитивність норми полягає не у обмеженій обов’язковій силі, а у тому, що вона передбачує право суб’єктів регулювати свої взаємовідносини інакше, ніж це передбачено загальною нормою. Специфіка таких норм полягає також у тому, що часто сторони, приймаючи їх залишають собі певну свободу вибору варіанту поведінки. Здійснений вибір є обов’язковим для сторін. |
| 3. | Рекомендаційними є норми, які покликані узгоджувати міжсуб’єктні відносини рекомендаційним способом, визначивши бажану, доцільну модель поведінки, але які не зобов’язують її виконувати. Такі норми мають суто юридичний характер, створюються відповідно до імперативних і диспозитивних норм і підпорядковані їм. |
| Концепція рекомендаційних норм міжнародного права породжена перш за все намаганнями пояснити природу резолюцій міжнародних організацій. При цьому ігнорується різниця двох явищ — рекомендаційних норм та рекомендацій як міжнародних актів. У першому випадку мова йде про норми, чиє призначення регулювати відносини рекомендаційним способом, встановлюючи бажану, доцільну модель поведінки, але на зобов’язуючи слідувати їй. У другому випадку маються на увазі акти, що мають силу рекомендацій, наприклад резолюції Генеральної Асамблеї ООН, які можуть містити категоричні приписи, але не мають юридичної сили. |

Концепція «м’якого права»

|  |  |  |
| --- | --- | --- |
| 1. | На сьогодні концепція «м’якого права» є недостатньо розробленою, оскільки ця дефініція використовується для позначення двох різних явищ. | |
| 1) | особливий вид міжнародно-правових норм; такі норми, які на відміну від, якщо можна так висловитися «твердого права», не породжують чітких прав та обов’язків, а надають лише загальну установку, якої, тим не менш, суб’єкти повинні дотримуватися. |
| У нових галузях міжнародно-правового регулювання нерідко вельми важко домогтися загальної згоди щодо конкретних норм. У такому разі на допомогу приходять норми «м’якого права», що відрізняються більшою гнучкістю. Прикладом можуть слугувати договори по захисту довкілля. У них використовуються формулювання в стилі «зроблять зусилля», «наскільки це можливо», коли це буде доцільним» тощо. |
| 2) | До другого виду норм «м’якого права» відносяться ті, що містять у не правових актах, у резолюціях міжнародних органів та організацій, у спільних заявах, комюніке. Про те, наскільки важливим може бути значення цих актів, свідчать, наприклад, рішення конференцій країн антигітлерівської коаліції. У наш час прикладом подібних норм слугують документи Організації з безпеки та співробітництва в Європі (ОБСЄ), які стали головним інструментом перебудови системи міжнародних відносин у Європі. Такого роду норми є не правовими, а морально-політичними. |
| Особливий різновид цього виду норм «м’якого права» становлять договори, що очікують набуття чинності. Як відому, у такому стані багатосторонні договори часто залишаються багато років поспіль. Їх положення враховуються при тлумаченні норм міжнародного права. У Доповіді Генерального секретаря МОП про конвенції цієї організації вказується на те, що такі конвенції навіть коли вони ще не ратифіковані можуть здійснювати вплив на законодавство та національну практику. |
| Норми «м’якого права» другого виду взаємодіють з нормами міжнародного права, виконуючи те, що з тих чи інших причин не можуть робити останні. Нерідко вони забезпечують попереднє, до правове регулювання, прокладаючи шлях праву. Особливо велике значення таких норм «м’якого права» для діяльності міжнародних органів та організацій, які з їх допомогою здійснюють великий об’єм регулювання міжнародних відносин і впливають на розвиток міжнародного права. |
| 2. | Таким чином, «м’яке право» являє собою закономірне явище, яке дозволяє забезпечити нормативне регулювання у тих випадках, коли за допомогою «твердого права» зробити це неможливо. Далеко не у всіх випадках право є оптимальний інструментом вирішення завдань. Багато коли результат може бути досягнутий з меншими затратами сил та енергії іншими нормативними засобами. | |
| Становить інтерес практика Суду ЄС. Суд включив у право ЄС принцип пропорційності. У відповідності з ним необхідність у специфічному правовому акті повинна бути завчасно ретельно проаналізована з тим, щоб визначити можливість використання менш жорстких засобів для досягнення того ж результату. | |

Основні та підпорядковані норми

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | а) | Існують два поняття процесуального права: | |
| широке | вузьке |
| мова йде про сукупність норм, що регулюють як правотворчий, так і правозастосовний процес. | мова йде про сукупність норм, що регулюють правозастосовний процес |
| б) | У ході роботи над проектом статей про відповідальність держав Комісія міжнародного права ООН застосовувала відоме теорії держави і права розподілення норм на: | |
| основні (первинні) | підпорядковані (вторинні) |
| безпосередньо регулюють поведінку суб’єктів | визначають наслідки невиконання зобов’язань, що витікають з основних норм. |
| 2. | Процесуальне право — нова галузь міжнародного права. Раніше існували окремі норми такого роду. Необхідність у підвищенні ефективності міжнародного права спонукала держави приділяти більше уваги процесу йог функціонування. Першочергове значення для формування процесуального права мало прийняття у 1969 році Віденської конвенції про право міжнародних договорів, значна частина постанов якої носить процесуальний характер, регламентуючи створення, дію та припинення договірних норм. Багато з цих постанов за аналогією застосовуються і до звичайних норм. | | |
| Важливе місце в процесуальному праві належить нормам права міжнародних організацій. Значення мають і загальні принципи права, які здебільшого є процесуальними (наприклад, ніхто не може бути суддею у власній справі, пріоритет спеціального закону по відношенню до загального тощо). | | |
| 3. | Для процесуального права, як і для міжнародного права у цілому, головне значення мають основні цілі та принципи, які визначають спрямованість процесів створення та здійснення міжнародного права. | | |
| Процесуальні норми мають специфічну санкцію. Створення чи здійснення матеріальних норм у порушення норм процесуальних у залежності від ступеню порушення тягне за собою оспорюваність чи недійсність створених норм чи результатів неправомірного застосування норм. | | |
| Процесуальне право відрізняється високим ступенем диспозитивності. Воно визначає лише загальні риси процесуальної діяльності. Свої процесуальні норми містить практично кожен договір. | | |

2.5 Міжнародна інформаційна безпека

Дослідження наукових підходів, і в першу чергу правових, до міжнародної інформаційної безпеки дозволяє стверджувати, що впродовж останніх десятиліть склалось загальне бачення і розуміння низки важливих і принципових питань цієї теми.

Фактично мова йде про два підходи, які лягли в основу і дозволили визначити основні положення сучасних концепцій. Особливістю є те, що будучи висловленими, вони відразу стали основою позицій держав і залишаються майже незмінними до теперішнього часу.

Спільні положення для двох концепцій розуміння проблем міжнародної інформаційної безпеки.

|  |  |
| --- | --- |
| Концепції розуміння проблем міжнародної інформаційної безпеки характеризуються однаковим усвідомленням і розумінням: | |
| 1) | місця і значення інформаційних технологій, їх взаємозв’язку в рамках інформаційного простору (кіберпростору), ролі в реалізації загальної концепції інформаційного суспільства |
| 2) | необхідності захисту найважливіших національних інфраструктур, глобальних інформаційно-комунікаційних мереж і систем, а також цілісності накопиченої інформації |
| 3) | складності, серйозності та чисельності загроз для інформаційно-комунікаційних технологій, пов’язаних як з процесами природнього і антропогенного характеру, так і діяльністю людини |
| 4) | неефективності традиційних стратегій (таких, як заходи, що аналогічно застосовуються в процесі контролю за озброєнням або їх стримування) |
| 5) | державних завдань, що постають на національному і міжнародному рівнях |
| 6) | необхідності об’єднання зусиль з метою збереження і розширення внеску, який ІКТ роблять у забезпечення безпеки і цілісності держав |
| 7) | необхідності міжнародної взаємодії в питанні розробки стратегій зменшення ризиків для ІКТ |
| До цього додається і спільна мета: створення глобальної культури кібербезпеки, сформульовану в рамках Організації Об'єднаних Націй. | |

Разом із тим привертають до себе увагу і розбіжності в концепціях. Мова йде про низку положень щодо принципів, структурних і функціональних елементів, місця міжнародної інформаційної безпеки.

Проблеми міжнародної інформаційної безпеки вперше в резолюції ГА ООН з акцентом на необхідності запобігання появи принципово нової - інформаційної - сфери конфронтації і розв'язання принципово нових конфліктів. (резолюції ГА ООН 53/70 "Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки" від 4 грудня 1998 року). Резолюція пропонує державам-членам ООН продовжити обговорення питань інформаційної безпеки, дати конкретні визначення загроз, запропонувати свої оцінки проблеми, включно з розробкою міжнародних принципів забезпечення безпеки глобальних інформаційних систем.

Резолюція ГА ООН 54/49 від 1 грудня 1999 року вперше вказала на загрози міжнародній інформаційній безпеці стосовно не тільки до цивільної, а й до військовій сфері.

У доповіді Генерального секретаря ООН від 10 червня 2000 року "Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки" відображені "Принципи, що стосуються міжнародної інформаційної безпеки".

Під інформаційною безпекою відповідно до Принципів розуміється стан захищеності основних інтересів особистості, суспільства і держави в інформаційному просторі, включаючи інформаційно-телекомунікаційну інфраструктуру і власне інформацію щодо таких її властивостей, як цілісність, об'єктивність, доступність і конфіденційність.

В подальшому, з огляду на резолюцію ГА ООН 55/28, що відзначає необхідність вивчення відповідних міжнародних концепцій, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем, була підготовлена доповідь Генерального секретаря ООН від 3 жовтня 2001 року "Про досягнення в сфері інформатизації та телекомунікації в контексті міжнародної безпеки ". В даному документі виділені 11 основних факторів, що створюють небезпеку для основних інтересів особистості, суспільства і держави в інформаційному просторі: розробка та використання коштів несанкціонованого втручання в роботу і неправомірного використання інформаційних ресурсів іншої держави, а також нанесення шкоди їм; цілеспрямований інформаційний вплив на критичні інфраструктури та населення іншої держави; дії, спрямовані на домінування в інформаційному просторі, заохочення тероризму, і власне ведення інформаційних війн і інше.

Резолюцією ГА ООН 56/19 від 29 листопада 2001 року схвалена ідея створення в 2004 році спеціальної Групи урядових експертів держав-членів ООН для проведення всебічного дослідження проблеми міжнародної інформаційної безпеки. Мандатом групи передбачається розгляд існуючих і потенційних загроз у сфері інформаційної безпеки і можливих спільних заходів щодо їх усунення, а також вивчення міжнародних концепцій, які були б спрямовані на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем.

Резолюція ГА ООН 62/17 від 5 грудня 2007 року закликає держав-членів і далі сприяти розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки, а також можливих заходів по обмеженню загроз, що виникають у цій сфері.

2.6 Правове забезпечення розвитку інформаційного суспільства: Окінавська Хартія глобального інформаційного суспільства

2.6.1 Текст Окінавської Хартії глобального інформаційного суспільства на сайті Верховної ради України, Прийняття від 22.07.2000

Окинавская хартия глобального информационного общества

(Окинава, 22 июля 2000 года)

1. Информационно-коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИТ быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы. Перед всеми нами открываются огромные возможности.

2. Суть стимулируемой ИТ экономической и социальной трансформации заключается в ее способности содействовать людям и обществу в использовании знаний и идей. Информационное общество, как мы его представляем, позволяет людям шире использовать свой потенциал и реализовывать свои устремления. Для этого мы должны сделать так, чтобы ИТ служили достижению взаимодополняющих целей обеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепления демократии, транспарентного и ответственного управления, прав человека, развития культурного многообразия и укрепления международного мира и стабильности. Достижение этих целей и решение возникающих проблем потребует разработки эффективных национальных и международных стратегий.

3. Стремясь к достижению этих целей, мы вновь подтверждаем нашу приверженность принципу участия в этом процессе: все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей.

4. Мы будем осуществлять руководство в продвижении усилий правительств по укреплению соответствующей политики и нормативной базы, стимулирующих конкуренцию и новаторство, обеспечение экономической и финансовой стабильности, содействующих сотрудничеству по оптимизации глобальных сетей, борьбе со злоупотреблениями, которые подрывают целостность сети, по сокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия и этом процессе.

5. Настоящая Хартия является прежде всего призывом ко всем как в государственном, так и в частном секторах ликвидировать международный разрыв в области информации и знаний. Солидная основа политики и действий в сфере ИТ может изменить методы нашего взаимодействия по продвижению социального и экономического прогресса во всем мире. Эффективное партнерство среди участников, включая совместное политическое сотрудничество, также является ключевым элементом рационального развития информационного общества.

Использование возможностей цифровых технологий

6. Потенциальные преимущества ИТ, стимулирующие конкуренцию, способствующие расширению производства, создающие и поддерживающие экономический рост и занятость, имеют значительные перспективы. Наша задача заключается не только в стимулировании и содействии переходу к информационному обществу, но также и в полной реализации его экономических, социальных и культурных преимуществ. Для достижения этих целей важно строить работу на следующих ключевых направлениях:

- проведение экономических и структурных реформ в целях создания обстановки открытости, эффективности, конкуренции и использования нововведений, которые дополнялись бы мерами по адаптации на рынках труда, развитию людских ресурсов и обеспечению социального согласия;

- рациональное управление макроэкономикой, способствующее более точному планированию со стороны деловых кругов и потребителей, и использование преимуществ новых информационных технологий;

- разработка информационных сетей, обеспечивающих быстрый, надежный, безопасный и экономичный доступ с помощью конкурентных рыночных условий и соответствующих нововведений к сетевым технологиям, их обслуживанию и применению;

- развитие людских ресурсов, способных отвечать требованиям века информации, посредством образования и пожизненного обучения и удовлетворение растущего спроса на специалистов в области ИТ во многих секторах нашей экономики;

- активное использование ИТ в государственном секторе и содействие предоставлению в режиме реального времени услуг, необходимых для повышения уровня доступности власти для всех граждан.

7. Частный сектор играет жизненно важную роль в разработке информационных и коммуникационных сетей в информационном обществе. Однако задача создания предсказуемой, транспарентной и недискриминационной политики и нормативной базы, необходимой для информационного общества, лежит на правительствах. Нам необходимо позаботиться о том, чтобы правила и процедуры, имеющие отношение к ИТ, соответствовали коренным изменениям в экономических сделках с учетом принципов эффективного партнерства между государственным и частным сектором, а также транспарентности и технологической нейтральности. Такие правила должны быть предсказуемыми и способствовать укреплению делового и потребительского доверия. В целях максимизации социальной и экономической выгоды информационного общества мы согласны со следующими основными принципами и подходами и рекомендуем их другим:

- продолжение содействия развитию конкуренции и открытию рынков для информационной технологии, и телекоммуникационной продукции, и услуг, включая недискриминационное и основанное на затратах подключение к основным телекоммуникациям;

- защита прав интеллектуальной собственности на информационные технологии имеет важное значение для продвижения нововведений, связанных с ИТ, развития конкуренции и широкого внедрения новых технологий; мы приветствуем совместную работу представителей органов власти по защите интеллектуальной собственности и поручаем нашим экспертам обсудить дальнейшие направления работы в этой сфере;

- важно также вновь подтвердить обязательство правительств использовать только лицензированное программное обеспечение;

- ряд услуг, включая телекоммуникации, транспорт, доставку посылок, имеют важное значение для информационного общества и экономики; повышение их эффективности и конкурентоспособности позволит расширить преимущества информационного общества; таможенные и экспедиторские процедуры также важны для развития информационных структур;

- развитие трансграничной электронной торговли путем содействия дальнейшей либерализации, улучшения сетей и соответствующих услуг и процедур в контексте жестких рамок Всемирной торговой организации (ВТО), продолжение работы в области электронной торговли в ВТО и на других международных форумах и применение существующих торговых правил ВТО к электронной торговле;

- последовательные подходы к налогообложению электронной торговли, основанные на обычных принципах, включая недискриминацию, равноправие, упрощенность и прочие ключевые элементы, согласованные в контексте работы Организации экономического сотрудничества и развития (ОЭСР);

- продолжение практики освобождения электронных переводов от таможенных пошлин до тех пор, пока она не будет рассмотрена вновь на следующей министерской конференции ВТО;

- продвижение рыночных стандартов, включая, например, технические стандарты функциональной совместимости;

- повышение доверия потребителя к электронным рынкам в соответствии с руководящими принципами ОЭСР, в том числе посредством эффективных саморегулирующих инициатив, таких как кодексы поведения, маркировка, другие программы подтверждения надежности, и изучение вариантов устранения сложностей, которые испытывают потребители в ходе трансграничных споров, включая использование альтернативных механизмов разрешения споров;

- развитие эффективного и значимого механизма защиты частной жизни потребителя, а также защиты частной жизни при обработке личных данных, обеспечивая при этом свободный поток информации; а также

- дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

8. Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства. Мы должны обеспечить осуществление эффективных мер - как это указано в Руководящих принципах по безопасности информационных систем ОЭСР - в борьбе с преступностью в компьютерной сфере. Будет расширено сотрудничество стран "Группы восьми" в рамках Лионской группы по транснациональной организованной преступности. Мы будем и далее содействовать установлению диалога с представителями промышленности, развивая, таким образом, успех, достигнутый на недавно прошедшей Парижской конференции "Группы восьми" "Диалог между правительством и промышленностью о безопасности и доверии в киберпространстве". Необходимо также найти эффективные политические решения актуальных проблем, как, например, попытки несанкционированного доступа и компьютерные вирусы. Мы будем и далее привлекать представителей промышленности и других посредников для защиты важных информационных инфраструктур.

Преодоление электронно-цифрового разрыва

9. Вопрос о преодолении электронно-цифрового разрыва внутри государств и между ними занял важное место в наших национальных дискуссиях. Каждый человек должен иметь возможность доступа к информационным и коммуникационным сетям. Мы подтверждаем нашу приверженность предпринимаемым в настоящее время усилиям по разработке и осуществлению последовательной стратегии, направленной на решение данного вопроса. Мы также приветствуем то, что и промышленность, и гражданское общество все более склоняются к признанию необходимости преодоления этого разрыва. Мобилизация наших знаний и ресурсов в этой области является необходимым условием для урегулирования данной проблемы. Мы будем и далее стремиться к эффективному сотрудничеству между правительствами и гражданским обществом, чутко реагирующим на высокие темпы развития технологий и рынка.

10. Ключевой составляющей нашей стратегии должно стать непрерывное движение в направлении всеобщего доступа для всех. Мы будем и далее:

- содействовать установлению благоприятных рыночных условий, необходимых для предоставления населению услуг в области коммуникаций;

- изыскивать дополнительные возможности, включая доступ через учреждения, открытые для широкой публики;

- уделять приоритетное внимание совершенствованию сетевого доступа, в особенности в отсталых городских, сельских и отдаленных районах;

- уделять особое внимание нуждам и возможностям людей, пользующихся меньшей социальной защищенностью, людей с ограниченной трудоспособностью, а также пожилых граждан, и активно осуществлять меры, направленные на предоставление им более легкого доступа;

- содействовать дальнейшему развитию "удобных для пользования", "беспрепятственных" технологий, включая мобильный доступ к сети Интернет, а также более широкое использование бесплатного, общедоступного информационного наполнения и открытых для всех пользователей программных средств, соблюдая при этом права на интеллектуальную собственность.

11. Стратегия развития информационного общества должна сопровождаться развитием людских ресурсов, возможности которых соответствовали бы требованиям информационного века. Мы обязуемся предоставить всем гражданам возможность освоить и получить навыки работы с ИТ посредством образования, пожизненного обучения и подготовки. Мы будем и далее стремиться к осуществлению этой масштабной цели, предоставляя школам, классам и библиотекам компьютерное оборудование, способное работать в режиме реального времени, а также направлять туда преподавателей, имеющих навыки работы с ИТ и мультимедийными средствами. Кроме того, мы будем осуществлять меры по поддержке и стимулированию малых и средних предприятий, а также людей, работающих не по найму, предоставляя им возможность подключаться к сети Интернет и эффективно ею пользоваться. Мы также будем поощрять использование ИТ в целях предоставления гражданам возможности пожизненного обучения с применением передовых методик, в особенности тем категориям граждан, которые в противном случае не имели бы доступа к образованию и профессиональной подготовке.

Содействие всеобщему участию

12. ИТ открывает перед развивающимися странами великолепные возможности. Страны, которым удалось направить свой потенциал в нужное русло, могут надеяться на преодоление препятствий, традиционно возникающих в процессе развития инфраструктуры, более эффективное решение своих насущных задач в области развития, таких как сокращение бедности, здравоохранение, улучшение санитарных условий и образование, а также использование преимуществ быстрого роста глобальной электронной торговли. Некоторые развивающиеся страны уже достигли значительных успехов в этих областях.

13. Тем не менее не стоит недооценивать проблему мирового масштаба, связанную с преодолением существующих различий в области информации и знаний. Мы отдаем должное тому вниманию, которое уделяют этой проблеме многие развивающиеся страны. В действительности, все те развивающиеся страны, которые не успевают за все более высокими темпами развития ИТ, оказываются лишенными возможности в полной мере участвовать в жизни информационного общества и экономике. Этот вопрос особенно остро стоит в тех странах, где распространению ИТ препятствует отставание в развитии основных экономических и социальных инфраструктур, в частности энергетического сектора, телекоммуникаций и образования.

14. Мы признаем, что при решении этой проблемы следует учитывать разнообразие условий и потребностей, которое сложилось в развивающихся странах. Здесь не может быть "уравнительного" решения. И это в свою очередь говорит о той важной роли, которую должны сыграть развивающиеся страны, выдвигая собственные инициативы о принятии последовательных национальных программ с целью осуществления политических мер, направленных на поддержку развития ИТ и конкуренции в этой сфере, а также создания нормативной базы, использование ИТ в интересах решения задач в области развития и в социальной сфере, развитие людских ресурсов, имеющих навыки работы с ИТ, а также с целью поощрения выдвигаемых на локальном уровне инициатив и местного предпринимательства.

Дальнейшее развитие

15. Усилия по преодолению международной разобщенности в решающей степени зависят от эффективного сотрудничества между всеми участниками. Для создания рамочных условий для развития ИТ важную роль и в дальнейшем будет играть двустороннее и многостороннее сотрудничество. Международные финансовые институты, включая многосторонние банки развития (МБР), особенно Всемирный банк, весьма пригодны для этой цели и могут разрабатывать и осуществлять программы, которые будут способствовать росту и борьбе с бедностью, а также расширять связи, доступ и обучение. Международная сеть телекоммуникаций, ЮНКТАД и ЮНДП и другие соответствующие международные фонды также могут сыграть важную роль. Центральной остается роль частного сектора в продвижении ИТ в развивающихся странах. Он может также существенно способствовать международным усилиям по преодолению цифрового разрыва. НПО, обладающие уникальными возможностями донести идеи до общественности, также могут способствовать развитию человеческих и общественных ресурсов. ИТ глобальна по своей сути и требует глобального подхода.

16. Мы приветствуем уже предпринимаемые усилия по преодолению международного электронно-цифрового разрыва посредством двусторонней помощи в области развития и по линии международных организаций и частных групп. Мы также приветствуем вклад частного сектора в лице таких организаций, как Глобальная инициатива по ликвидации электронно-цифрового разрыва Всемирного экономического форума (ВЭФ) и Глобальный диалог бизнеса по вопросам электронной торговли (ГДБ), а также Глобальный форум.

17. Как отмечается в Декларации о роли информационных технологий в контексте основанной на знаниях глобальной экономики, которая была принята Экономическим и Социальным Советом ООН (ЭКОСОС) на уровне министров, существует необходимость расширения международного диалога и сотрудничества в целях повышения эффективности программ и проектов в области информационных технологий совместно с развивающимися странами и сведения воедино "наилучшего опыта", а также мобилизации ресурсов всех участников для того, чтобы способствовать ликвидации электронно-цифрового разрыва. "Восьмерка" будет и далее содействовать укреплению партнерства между развитыми и развивающимися странами, гражданским обществом, включая частные фирмы и НПО, фонды и учебные заведения, а также международные организации. Мы будем также работать над тем, чтобы развивающиеся страны в партнерстве с другими участниками могли получать финансовое, техническое и политическое обеспечение в целях создания благоприятного климата для использования информационных технологий.

18. Мы договорились об учреждении Группы по возможностям информационной технологии (Группа ДОТ), чтобы объединить наши усилия в целях формирования широкого международного подхода. Группа ДОТ будет созвана в кратчайшие сроки для изучения наилучших возможностей подключения к работе всех участников. Эта группа высокого уровня в режиме тесных консультаций с другими партнерами и воспринимая потребности развивающихся стран будет:

- активно содействовать диалогу с развивающимися странами, международными организациями и другими участниками для продвижения международного сотрудничества с целью формирования политического, нормативного и сетевого обеспечения, а также улучшения технической совместимости, расширения доступа, снижения затрат, укрепления человеческого потенциала, а также поощрения участия в глобальных сетях электронной торговли;

- поощрять собственные усилия "восьмерки" в целях сотрудничества в осуществлении экспериментальных программ и проектов в области информационных технологий;

- содействовать более тесному политическому диалогу между партнерами и работать над тем, чтобы мировая общественность больше знала о стоящих перед ней вызовах и имеющихся возможностях;

- изучит вопрос о том, какой вклад вносит частный сектор и другие заинтересованные группы, например, Глобальная инициатива по ликвидации электронно-цифрового разрыва;

- представит доклад по итогам работы нашим личным представителям до следующей встречи в Генуе.

19. Для выполнения этих задач группа будет изыскивать пути к принятию конкретных мер в указанных ниже приоритетных областях:

формирование политического, нормативного и сетевого обеспечения:

- поддержка политического консультирования и укрепление местного потенциала, с тем чтобы способствовать проведению направленной на создание конкуренции гибкой и учитывающей социальные аспекты политики, а также нормативному обеспечению;

- содействие обмену опытом между развивающимися странами и другими партнерами;

- содействие более эффективному и широкому использованию информационных технологий в области развития, включая такие широкие направления, как сокращение бедности, образование, здравоохранение и культура;

- совершенствование системы управления, включая изучение новых методов комплексной разработки политики;

- поддержка усилий МБР и других международных организаций в целях объединения интеллектуальных и финансовых ресурсов в контексте программ сотрудничества, таких как программа "InfoDev".

улучшение технической совместимости, расширение доступа и снижение затрат:

- мобилизация ресурсов в целях улучшения информационной и коммуникационной инфраструктуры, уделение особого внимания "партнерскому" подходу со стороны правительств, международных организаций, частного сектора и НПО;

- поиск путей снижения затрат для развивающихся стран в обеспечении технической совместимости;

- поддержка программ доступа на местном уровне;

- поощрение технологических исследований и прикладных разработок в соответствии с конкретными потребностями развивающихся стран;

- улучшение взаимодействия между сетями, службами и прикладными системами;

- поощрение производства современной информационно-содержательной продукции, включая расширение объема информации на родных языках.

- укрепление человеческого потенциала:

- уделение повышенного внимания базовому образованию, а также расширению возможностей пожизненного обучения с упором на развитие навыков использования информационных технологий;

- содействие подготовке специалистов в сфере информационных технологий и других актуальных областях, а также в нормативной сфере;

- разработка инновационных подходов в целях расширения традиционной технической помощи, включая дистанционное обучение и подготовку на местном уровне;

- создание сети государственных учреждений и институтов, включая школы, научно-исследовательские центры и университеты.

поощрение участия в работе глобальных сетей электронной торговли

- оценка и расширение возможностей использования электронной торговли посредством консультирования при открытии бизнеса в развивающихся странах, а также путем мобилизации ресурсов в целях содействия предпринимателям в использовании информационных технологий для повышения эффективности их деятельности и расширения доступа к новым рынкам.

2.6.2 Характеристики інформаційного суспільства, що відображені в Окинавській хартії

Okinawa Charter on Global Information Society, 22 липня 2000 року на офіційному сайті МЗС Японії. Підписана главами держав «сімки» на Окінаві.

|  |  |
| --- | --- |
| Глобальне інформаційне суспільство: | |
| 1. | наявність інформаційної інфраструктури - транскордонних інформаційно-телекомунікаційних мереж (ТІТМ) |
| 2. | масове застосування ПК, підключених до ТІТМ |
| 3. | підготовленість членів суспільства до роботи на ПК і в ТІТМ |
| 4. | нові форми і види діяльності в ТІТМ (повсякденна трудова діяльність в мережах, купівля-продаж товарів і послуг, зв'язок і комунікація, відпочинок і розвага, медичне обслуговування і т.п.) |
| 5. | можливість кожному миттєво отримувати з ТІТМ повну, точну і достовірну інформацію |
| 6. | миттєва комунікація кожного члена суспільства з кожним, кожного з усіма і всіх з кожним |
| 7. | трансформація діяльності ЗМІ, інтеграція ЗМІ і ТІТМ, створення єдиного середовища поширення масової інформації - мультимедіа |
| 8. | відсутність географічних і геополітичних кордонів держав - учасниць ТІТМ, «зіткнення» національних законодавств країн, становлення нового міжнародного інформаційного права і законодавства |

2.7 Конвенція про кіберзлочинність

Конвенція про кіберзлочинність

Преамбула

Розділ I - Використання термінів

Стаття 1 - Визначення

Для цілей цієї Конвенції:

a. "комп'ютерна система" означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних;

b. "комп'ютерні дані" означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

c. "постачальник послуг" означає:

i. будь-яку державну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та

ii. будь-яку іншу установу, яка обробляє або зберігає комп'ютерні дані від імені такої комунікаційної послуги або користувачів такої послуги.

d. "дані про рух інформації" означає будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги.

Розділ II - Заходи, які мають здійснюватися на національному рівні

Частина 1 - Матеріальне кримінальне право

Заголовок 1- Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Стаття 2 - Незаконний доступ

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 3 - Нелегальне перехоплення

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 4 - Втручання у дані

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це.

2. Сторона може залишити за собою право вимагати, щоб поведінка, описана у пункті 1, завдавала серйозну шкоду.

Стаття 5 - Втручання у систему

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

Стаття 6 - Зловживання пристроями

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це:

a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином:

i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5 вище;

ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи

з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5; та

b. володіння предметом, перерахованим у підпунктах a.i або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів.

2. Ця стаття не тлумачиться як така, що встановлює кримінальну відповідальність у разі, якщо виготовлення, продаж, придбання для використання, розповсюдження чи надання для використання іншим чином або володіння, зазначені у пункті 1 цієї статті, не призначені для вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5 цієї Конвенції, такі як дозволене випробування або захист комп'ютерної системи.

3. Кожна Сторона може залишити за собою право не застосовувати пункт 1 цієї статті, за умови, що таке застереження не стосується продажу, розповсюдження або надання для використання іншим чином предметів, перерахованих у підпункті 1.a.ii цієї статті.

Заголовок 2 - Правопорушення, пов'язані з комп'ютерами

Стаття 7 - Підробка, пов'язана з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності.

Стаття 8 - Шахрайство, пов'язане з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних,

b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.

Заголовок 3 - Правопорушення, пов'язані зі змістом Стаття 9 - Правопорушення, пов'язані з дитячою порнографією

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій:

a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;

b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;

c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;

d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;

e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

2. Для цілей пункту 1 вище "дитяча порнографія" включає в себе порнографічний матеріал, який візуально зображує:

a. неповнолітню особу, задіяну у явно сексуальній поведінці;

b. особу, яка виглядає як неповнолітня особа, задіяну у явно сексуальній поведінці;

c. реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці.

3. Для цілей пункту 2 вище термін "неповнолітня особа" включає в себе усіх осіб до 18 років. Сторона може, однак, передбачити нижчий віковий поріг, який має бути не меншим за 16 років.

4. Кожна Сторона може залишити за собою право не застосовувати, частково чи повністю, підпункти 1.d, 1.e, 2.b та 2.c.

Заголовок 4 - Правопорушення, пов'язані з порушенням авторських та суміжних прав

Стаття 10 - Правопорушення, пов'язані з порушенням авторських та суміжних прав

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів ( 995\_051 ), Угодою про торгівельні аспекти прав інтелектуальної власності ( 981\_018 ) і Угодою ВОІВ про авторське право ( 995\_770 ), за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення ( 995\_763 ) (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності ( 981\_018 ) і Угодою ВОІВ про виконання і фонограми ( 995\_769 ), за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

3. Кожна Сторона може залишити за собою право не встановлювати кримінальну відповідальність відповідно до пунктів 1 і 2 цієї статті у обмежених випадках, за умови існування інших ефективних засобів впливу, і за умови того, що таке застереження не порушує міжнародних зобов'язань Сторони відповідно до міжнародних документів, на які містяться посилання у пунктах 1 і 2 цієї статті.

Заголовок 5 - Додаткова відповідальність і санкції

Стаття 11 - Спроба і допомога або співучасть

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів, перерахованих у статтях 2 - 10 цієї Конвенції, з метою вчинення такого злочину.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисну спробу вчинити будь-який зі злочинів, перерахованих у статтях 3 - 5, 7, 8, 9.1.a та 9.1.c цієї Конвенції.

3. Кожна Сторона може залишити за собою право не застосовувати, повністю чи частково, пункт 2 цієї Статті.

Стаття 12 - Корпоративна відповідальність

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи. Така фізична особа має займати керівну посаду в рамках юридичної особи, в силу:

a. повноважень представляти цю юридичну особу;

b. повноважень приймати рішення від імені цієї юридичної особи;

c. повноважень здійснювати контроль в рамках цієї юридичної особи.

2. На додаток до випадків, вже передбачених у пункті 1 цієї статті, кожна Сторона вживає заходів для забезпечення того, щоб юридична особа могла понести відповідальність у разі, коли недостатній нагляд чи контроль, який мав здійснюватися особою, вказаною у пункті 1, створив можливість вчинення кримінального правопорушення, встановленого відповідно до цієї Конвенції, на користь такої юридичної особи фізичною особою, яка діяла під її контролем.

3. Відповідно до юридичних принципів Сторони, відповідальність юридичної особи може бути кримінальною, цивільною або адміністративною.

4. Така відповідальність не впливає на кримінальну відповідальність фізичних осіб, які вчинили правопорушення.

Стаття 13 - Санкції і заходи

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб кримінальні правопорушення, встановлені відповідно до статей 2 - 11, каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі.

2. Кожна Сторона забезпечує, щоб юридичні особи, які несуть відповідальність відповідно до статті 12, каралися ефективними, пропорційними і переконливими кримінальними або некримінальними санкціями або заходами, включаючи грошові санкції.

Частина 2 - Процедурне право

Заголовок 1 - Загальні положення

Стаття 14 - Сфера процедурних положень

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань.

2. За винятком обставин, конкретно передбачених статтею 21, кожна Сторона застосовує повноваження і процедури, передбачені у пункті 1 цієї статті, до:

a. кримінальних правопорушень, встановлених відповідно до статей 2 - 11 цієї Конвенції;

b. інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем; та

c. збору доказів у електронній формі стосовно кримінального правопорушення.

3. a. Кожна Сторона може залишити за собою право застосовувати заходи, які містяться у статті 20, тільки до правопорушень або до категорій правопорушень, зазначених у застереженні, за умови, що обсяг таких правопорушень або категорій правопорушень не менший за обсяг правопорушень, до яких вона застосовує заходи, які містяться у статті 21. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статті 20.

b. Якщо Сторона внаслідок обмежень, встановлених її чинним законодавством під час прийняття цієї Конвенції, не може застосовувати заходи, які містяться у статтях 20 і 21, до комунікацій, які передаються всередині комп'ютерної системи постачальника послуг, причому така система

i. використовується на користь закритої групи користувачів, та

ii. не використовує мережі зв'язку загального доступу, і не пов'язана з іншою комп'ютерною системою, відкритою для загального доступу чи приватною,

така Сторона може залишити за собою право не застосовувати ці заходи для таких комунікацій. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статтях 20 і 21.

Стаття 15 - Умови і запобіжні заходи

1. Кожна Сторона забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, передбачених цією частиною, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини, включаючи права, що випливають із зобов'язань за Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р. ( 995\_004 ), Міжнародною Хартією ООН про громадянські і політичні права 1966 р. ( 995\_043 ), та інших відповідних міжнародних угод з прав людини, і які б включали в себе принцип пропорційності.

2. Такі умови і запобіжні заходи включатимуть, між іншим, як це є доречним з огляду на природу відповідного повноваження або процедури, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур.

3. У тій мірі, наскільки це відповідає суспільним інтересам, зокрема, належному відправленню правосуддя, кожна Сторона розгляне вплив повноважень і процедур, які містяться у цій частині, на права, відповідальність і законні інтереси третіх сторін.

Заголовок 2 - Загальні положення

Стаття 16 - Термінове збереження комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання можливості своїм компетентним органам видавати ордери або іншим подібним шляхом спричиняти термінове збереження визначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у випадку, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації.

2. Якщо Сторона застосовує пункт 1 вище шляхом видачі ордеру особі, яким така особа зобов'язується зберігати визначені комп'ютерні дані, які зберігаються і знаходяться у власності або під контролем такої особи, вона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати таку особу зберігати і підтримувати цілісність таких комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їхнє розкриття, з максимальним терміном у 90 днів. Сторона може передбачити можливість наступного продовження терміну дії такого ордеру.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати особу, яка має зберігати комп'ютерні дані, зберігати конфіденційність факту проведення таких процедур протягом періоду, визначеного її внутрішньодержавним законодавством.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Стаття 17 - Термінове збереження і часткове розкриття даних про рух інформації

1. Кожна Сторона вживає по відношенню до даних про рух інформації, які мають зберігатися відповідно до статті 16, такі законодавчі та інші заходи, які можуть бути необхідними для:

a. забезпечення того, щоб таке термінове збереження даних про рух інформації могло проводитися, незважаючи на те, один чи більше постачальників послуг було залучено до передачі такої інформації; та

b. забезпечити термінове розкриття компетентному органові Сторони або особі, призначеній таким органом, обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг і маршруту, яким була передана інформація.

2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Заголовок 3 - Порядок представлення

Стаття 18 - Порядок представлення

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати ордери:

a. особі, яка знаходиться на її території - про надання зазначених комп'ютерних даних, якими така особа володіє або контролює, і які зберігаються у комп'ютерній системі або на комп'ютерному носії інформації; та

b. постачальнику послуг, який пропонує свої послуги на території Сторони - про надання інформації про користувача послуг, пов'язаної з такими послугами, яка знаходиться у власності або під контролем такого постачальника послуг.

2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

3. Для цілей цієї статті термін "інформація про користувача послуг" означає будь-яку інформацію, у формі комп'ютерних даних чи у іншій формі, яка знаходиться у постачальника послуг, відноситься до користувачів його послуг, не є даними про рух даних або власне даними змісту інформації, та за допомогою якої можна встановити:

a. тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;

b. особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг;

c. будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про постачання послуг.

Заголовок 4 - Обшук і арешт комп'ютерних даних, які зберігаються

Стаття 19 - Обшук і арешт комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам для обшуку або подібного доступу до:

a. комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній; та

b. комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані на її території.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб у випадку, коли її компетентні органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини відповідно до підпункту 1.a, і мають підстави вважати, що дані, які розшукуються, зберігаються у іншій комп'ютерній системі чи її частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ з першої системи чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень арештовувати або вчиняти подібні дії щодо комп'ютерних даних, до яких був здійснений доступ відповідно до пунктів 1 або 2. Такі заходи включатимуть повноваження на:

a. арешт або подібні дії щодо комп'ютерної системи або її частини або комп'ютерного носія інформації;

b. копіювання і збереження копії таких комп'ютерних даних;

c. збереження цілісності відповідних збережених комп'ютерних даних;

d. заборону доступу або вилучення цих комп'ютерних даних з комп'ютерної системи, до якої здійснювався доступ.

4. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень вимагати від будь-якої особи, яка знає про функціонування комп'ютерної системи або про заходи, які були здійснені для захисту комп'ютерних даних, які містяться у ній, надавати, наскільки це можливо, необхідну інформацію для проведення дій, які містяться у пунктах 1 і 2.

5. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Заголовок 5 - Збирання комп'ютерних даних у реальному масштабі часу

Стаття 20 - Збирання даних про рух інформації у реальному масштабі часу

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень:

a. збирати або записувати технічними засобами на території такої Сторони, та

b. зобов'язувати постачальника послуг, в межах його існуючих технічних можливостей:

i. збирати або записувати технічними засобами на території такої Сторони; або

ii. співробітничати і допомагати компетентним органам у зборі або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, яка передається за допомогою комп'ютерних систем.

2. Якщо Сторона, в силу встановлених принципів її юридичної системи, не може застосувати заходи, на які містяться посилання у пункті 1.a, вона замість цього може вжити такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення збору або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту використання будь-якого з повноважень, зазначених у цій статті, і будь-якої інформації, пов'язаної з цим.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Стаття 21 - Перехоплення даних змісту інформації

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними стосовно певних серйозних злочинів, які визначаються внутрішньодержавним законодавством, для надання повноважень своїм компетентним органам:

a. збирати або записувати технічними засобами на території такої Сторони, або

b. зобов'язувати постачальника послуг, в межах його існуючих технічних можливостей:

i. збирати або записувати технічними засобами на території такої Сторони; або

ii. співробітничати і допомагати компетентним органам у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється за допомогою комп'ютерних систем.

2. Якщо Сторона, в силу встановлених принципів її юридичної системи, не може застосувати заходи, на які містяться посилання у пункті 1.a, вона замість цього може вжити такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення збору або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту використання будь-якого з повноважень, зазначених у цій статті, і будь-якої інформації, пов'язаної з цим.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Частина 3 - Юрисдикція

Стаття 22 - Юрисдикція

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, встановленого відповідно до статей 2 - 11 цієї Конвенції, у випадках, коли таке правопорушення вчинене:

a. на її території; або

b. на борту судна, яке плаває під прапором такої Сторони; або

c. на борту літака, зареєстрованого відповідно до законодавства такої Сторони; або

d. одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

2. Кожна Держава може залишити за собою право не застосовувати або застосовувати лише у окремих випадках або за окремих умов правила юрисдикції, викладені у пунктах 1.b - 1.d цієї статті або у будь-якій їх частині.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення юрисдикції стосовно злочинів, встановлених відповідно до пункту 1 статті 24 цієї Конвенції, у випадках, коли підозрюваний правопорушник знаходиться на її території, і після запиту про екстрадицію не передається іншій Стороні лише на підставі його громадянства.

4. Ця Конвенція не виключає будь-якої кримінальної юрисдикції, яка здійснюється Стороною відповідно до її внутрішньодержавного законодавства.

5. Якщо більш ніж одна Сторона заявляє про юрисдикцію стосовно підозрюваного правопорушення, встановленого відповідно до цієї Конвенції, заінтересовані Сторони, де це можливо, проводять консультації з метою визначення найбільш придатної для переслідування юрисдикції.

Розділ III - Міжнародне співробітництво

Частина 1 - Загальні принципи

Заголовок 1 - Загальні принципи міжнародного співробітництва

Стаття 23 - Загальні принципи міжнародного співробітництва

Сторони співробітничають між собою у найширших обсягах відповідно до принципів цього розділу шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Заголовок 2 - Принципи екстрадиції

Стаття 24 - Екстрадиція

1. a. Ця стаття застосовується до екстрадиції, що має місце між Сторонами у зв'язку з кримінальними правопорушеннями, встановленими відповідно до статей 2 - 11 цієї Конвенції, за умови, що вони підлягають покаранню позбавленням волі, максимальний строк якого складає щонайменше один рік, або більш суворому покаранню, відповідно до законодавства обох заінтересованих Сторін.

b. У випадках, коли відповідно до домовленості, укладеної на основі єдиного чи взаємного законодавства, або договору про екстрадицію, включаючи Європейську Конвенцію про екстрадицію (ETS N 24) ( 995\_033 ), які застосовуються між двома або більше сторонами, має застосовуватися різне мінімальне покарання, застосовується мінімальне покарання відповідно до такої домовленості чи угоди.

2. Кримінальні правопорушення, описані у пункті 1 цієї статті, вважаються такими, що включаються як правопорушення, які спричиняють екстрадицію, до будь-якої угоди про екстрадицію, яка існує між Сторонами. Сторони зобов'язуються включати такі правопорушення, як такі, що спричиняють екстрадицію, до будь-якого договору про екстрадицію, який буде укладено між ними.

3. Якщо Сторона, яка здійснює екстрадицію за умови існування договору, отримує запит про екстрадицію від іншої Сторони, з якою в неї нема договору про екстрадицію, вона може вважати цю Конвенцію юридичною основою для екстрадиції відносно будь-якого кримінального правопорушення, на яке міститься посилання у пункті 1 цієї статті.

4. Сторони, які не ставлять існування договору умовою для екстрадиції, визнають для себе кримінальні правопорушення, на які міститься посилання у пункті 1 цієї статті, такими, що спричиняють екстрадицію.

5. Екстрадиція підлягає умовам, передбаченим законодавством Сторони, яку запитують про екстрадицію, або відповідними договорами про екстрадицію, включаючи підстави, на яких Сторона, яку запитують, може відмовити в екстрадиції.

6. Якщо в екстрадиції стосовно кримінального правопорушення, на яке міститься посилання у пункті 1 цієї статті, відмовлено виключно на підставі громадянства особи, стосовно якої надходить запит про екстрадицію, або тому, що Сторона, яку запитують, вважає, що вона має юрисдикцію стосовно такого правопорушення, Сторона, яку запитують, на запит Сторони, яка запитує, надсилає справу своїм компетентним органам з метою переслідування правопорушення, і належним чином повідомляє його результат Стороні, яка запитує. Такі органи приймають свої рішення і проводять свої розслідування і переслідування таким же чином, як і у випадку будь-якого іншого правопорушення подібної природи відповідно до законодавства такої Сторони.

7. a. Кожна Сторона під час підписання або передачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання повідомляє Генеральному секретарю Ради Європи назви і адреси усіх компетентних органів, які відповідають за надсилання чи отримання запитів про екстрадицію або тимчасовий арешт у випадку відсутності договору.

b. Генеральний секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно призначених Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

Заголовок 3 - Загальні принципи взаємної допомоги

Стаття 25 - Загальні принципи взаємної допомоги

1. Сторони надають одна іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для виконання зобов'язань, що містяться у статтях 27 - 35.

3. Кожна Сторона за надзвичайних умов може зробити запит про взаємну допомогу або про повідомлення, пов'язані з такою допомогою, які здійснюються терміновими засобами комунікації, включаючи факс і електронну пошту, у тому обсязі, в якому такі засоби комунікацій можуть забезпечити належні форми безпеки і підтвердження достовірності (включаючи використання кодування, де це необхідно), за яким має слідувати формальне підтвердження, якщо таке вимагається Стороною, яку запитують. Сторона, яку запитують, приймає і відповідає на запит шляхом будь-якого з таких термінових засобів комунікації.

4. Якщо інше не передбачене статтями цього розділу, взаємна допомога надається відповідно до законодавства Сторони, яку запитують, або до відповідних договорів про взаємну допомогу, включаючи підстави, на яких Сторона, яку запитують, може відмовити у співробітництві. Сторона, яку запитують, не використовує право відмовити у взаємній допомозі відносно правопорушень, які містяться у статтях 2 - 11, тільки на підставі того, що запит стосується правопорушення, яке вона вважає фіскальним правопорушенням.

5. У разі, якщо відповідно до положень цього розділу, Стороні, яку запитують, дозволяється надавати взаємну допомогу за умови існування подвійного визнання правопорушення, ця умова вважається виконаною, незалежно від того, чи відносить її законодавство таке правопорушення до тієї ж категорії правопорушень або визначає його тією ж термінологією, як і Сторона, яка запитує, у разі, якщо поведінка, яка визначає правопорушення, стосовно якого запитується допомога, є кримінальним правопорушенням відповідно до законодавства Сторони, яку запитують.

Стаття 26 - Добровільно надана інформація

1. Сторона може в рамках свого законодавства без попереднього запиту надіслати іншій Стороні інформацію, отриману в ході її власного розслідування, якщо вона вважає, що розкриття такої інформації може допомогти Стороні, яка отримує інформацію, у відкритті або проведенні розслідування чи переслідування стосовно кримінальних злочинів, встановлених відповідно до цієї Конвенції або може спричинити запит про співробітництво від такої Сторони відповідно до цього розділу.

2. До надання такої інформації Сторона, яка надає інформацію, може вимагати, щоб вона залишалася конфіденційною або використовувалася за певних умов. Якщо Сторона, яка отримує інформацію, не може задовольнити вимоги такого запиту, вона повідомляє про це Сторону, яка надає інформацію, яка після цього визначає, чи надавати інформацію, незважаючи на це. Якщо Сторона, яка отримує інформацію, приймає її за певних умов, вона має їх дотримуватися.

Заголовок 4 - Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод

Стаття 27 - Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод

1. У разі відсутності між Стороною, яка запитує, і Стороною, яку запитують, чинних договорів про взаємну допомогу чи угод на основі єдиного чи взаємного законодавства, застосовуються положення пунктів 2 - 10 цієї статті. Положення цієї статті не застосовуються у разі наявності такого договору, угоди або законодавства, якщо тільки заінтересовані Сторони не погоджуються застосовувати замість них, частково або повністю, нижчевикладені положення цієї статті.

2. a. Кожна Сторона призначає центральний уповноважений орган або органи, які відповідають за надсилання та відповідь на запити про взаємну допомогу, виконання таких запитів або їх передачу уповноваженим органам, компетентним виконувати їх.

b. Ці центральні уповноважені органи здійснюють прямі зносини між собою.

c. Кожна Сторона під час підписання або передачі на зберігання ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання повідомляє Генеральному секретарю Ради Європи назви і адреси усіх компетентних органів, призначених відповідно до цього пункту.

d. Генеральний секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно призначених Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

3. Запити про взаємну допомогу відповідно до цієї статті здійснюються згідно процедур, зазначених Стороною, яка запитує, якщо тільки вони не суперечать законодавству Сторони, яку запитують.

4. Сторона, яку запитують, може, на додаток до підстав для відмови, передбачених у пункті 4 статті 25, відмовити у допомозі, якщо:

a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

b. вона вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

5. Сторона, яку запитують, може відкласти свої дії щодо запиту, якщо такі дії можуть зашкодити кримінальному розслідуванню чи переслідуванню, яке здійснюється її уповноваженими органами.

6. До відмови або відкладення допомоги Сторона, яку запитують, після консультацій з Стороною, яка запитує, розгляне, якщо це доречно, можливість часткового задоволення запиту або його задоволення за умов, які вона вважає доречними.

7. Сторона, яку запитують, терміново інформує Сторону, яка запитує, про результат виконання запиту про допомогу. Якщо у допомозі відмовлено чи вона відкладена, надаються причини відмови чи відкладення. Сторона, яку запитують, також інформує Сторону, яка запитує, про будь-які причини, які унеможливлюють виконання запиту або можуть значною мірою затримати його виконання.

8. Сторона, яка запитує, може вимагати від Сторони, яку запитують, зберігати конфіденційним факт і зміст будь-якого запиту, зробленого відповідно до цього розділу, за винятком того обсягу, який є необхідним для виконання запиту. Якщо Сторона, яку запитують, не може виконати запит за умов його конфіденційності, вона терміново інформує про це Сторону, яка запитує, яка після цього визначає, чи необхідно виконати запит, незважаючи на це.

9. a. У термінових випадках запити про взаємну допомогу або про повідомлення, пов'язані з нею, можуть надсилатися безпосередньо судовими органами Сторони, яка запитує, до відповідних органів Сторони, яку запитують. В будь-якому такому випадку копія одночасно надсилається центральному уповноваженому органу Сторони, яку запитують, через центральний уповноважений орган Сторони, яка запитує.

b. Будь-який запит або повідомлення відповідно до цього пункту може здійснюватися через Міжнародну організацію кримінальної поліції (Інтерпол).

c. Якщо запит здійснено відповідно до підпункту a. цієї статті, і орган не має компетенції розглядати такий запит, він передає запит до компетентного національного органу, і безпосередньо повідомляє про це Сторону, яка запитує.

d. Запити або повідомлення, здійснені відповідно до цього пункту, які не стосуються примусових дій, можуть передаватися безпосередньо компетентними органами Сторони, яка запитує, компетентним органам Сторони, яку запитують.

e. Кожна Сторона під час підписання або передачі на зберігання ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання може повідомити Генерального секретаря Ради Європи про те, що з метою ефективності усі запити відповідно до цього пункту мають надсилатися її центральному органу.

Стаття 28 - Конфіденційність і обмеження у використанні

1. У разі відсутності між Стороною, яка запитує, і Стороною, яку запитують, чинних договорів про взаємну допомогу чи угод на основі єдиного чи взаємного законодавства, застосовуються положення цієї статті. Положення цієї статті не застосовуються у разі наявності такого договору, угоди або законодавства, якщо тільки зацікавлені Сторони не погоджуються застосовувати замість них, частково або повністю, нижчевикладені положення цієї статті.

2. Сторона, яку запитують, може ставити умовою для надання інформації або матеріалів у відповідь на запит, вимогу, що таке надання інформації:

a. залишиться конфіденційним, якщо запит про взаємну правову допомогу не можна було б виконати за відсутності такої умови, або

b. не використовуватиметься для розслідувань або переслідувань, що не зазначені у запиті.

3. Якщо Сторона, яка запитує, не може виконати умову, що міститься у пункті 2, вона терміново інформує про це іншу Сторону, яка після цього визначає, чи може інформація бути надана, незважаючи на це. Якщо Сторона, яка запитує, приймає умову, вона є обов'язковою для неї.

4. Будь-яка Сторона, яка надає інформацію або матеріали за умови, що міститься у пункті 2, може вимагати, щоб інша Сторона надала пояснення про використання такої інформації у зв'язку із такою умовою.

Частина 2 - Конкретні принципи

Заголовок 1 - Взаємна допомога щодо тимчасових заходів

Стаття 29 - Термінове збереження комп'ютерних даних, які зберігаються

1. Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

2. У запиті про збереження відповідно до пункту 1 зазначається:

a. компетентний орган, який робить запит про збереження;

b. правопорушення, яке підлягає кримінальному розслідуванню або переслідуванню, і короткий опис відповідних фактів;

c. комп'ютерні дані, які необхідно зберегти, та їх зв'язок з правопорушенням;

d. будь-яка доступна інформація для ідентифікації особи, яка зберігає такі комп'ютерні дані, або розташування комп'ютерної системи;

e. необхідність збереження; та

f. положення про те, що така Сторона має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких комп'ютерних даних, які зберігаються.

3. Після отримання запиту від іншої Сторони, Сторона, яку запитують, вживає усіх належних заходів для термінового збереження зазначених даних відповідно до її внутрішньодержавного законодавства. Для цілей відповіді на запит, подвійне визнання правопорушення не вимагається як підстава для проведення такого збереження.

4. Сторона, яка вимагає подвійне визнання правопорушення як умову виконання запиту про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних, може відносно правопорушень, які не є правопорушеннями, встановленими статтями 2 - 11 цієї Конвенції, зберегти за собою право відмовити у виконанні запиту про збереження відповідно до цієї статті у випадках, коли вона має підстави вважати, що на час розголошення умову щодо подвійного визнання правопорушення не можна задовольнити.

5. На додаток до цього, у виконанні запиту про збереження можна відмовити лише у випадках, коли:

a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

b. Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

6. Якщо Сторона, яку запитують, вважає, що таке збереження не забезпечить майбутню доступність даних або загрожуватиме їх конфіденційності чи іншим чином зашкодить розслідуванню, яке проводить Сторона, яка запитує, вона терміново інформує про це Сторону, яка запитує. Після цього остання визначає, чи необхідно виконувати запит, незважаючи на це.

7. Будь-яке збереження, проведене у відповідь на запит відповідно до пункту 1, продовжується не менше ніж 60 днів, для того, щоб надати можливість Стороні, яка запитує, надіслати запит щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних. Після отримання такого запиту, дані зберігаються до винесення рішення стосовно такого запиту.

Стаття 30 - Термінове розкриття збережених даних про рух інформації

1. Якщо в ході виконання запиту, зробленого відповідно до статті 29, щодо збереження даних про рух інформації, які стосуються конкретної передачі інформації, Стороні, яку запитують, стає відомо, що постачальник послуг в іншій Державі був залучений до передачі такої інформації, Сторона, яку запитують, терміново повідомляє Стороні, яка запитує, обсяг інформації про рух даних, достатній для ідентифікації такого постачальника послуг і шляху передачі такої інформації.

2. У розкритті інформації про рух даних відповідно до пункту 1 може бути відмовлено тільки якщо:

a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

b. Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

Заголовок 2 - Взаємна допомога щодо повноважень розслідування

Стаття 31 - Взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються

1. Будь-яка Сторона може запитати іншу Сторону провести обшук чи подібний доступ, арешт чи подібні дії або розголошення даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території Сторони, яку запитують, включаючи дані, збережені відповідно до статті 29.

2. Сторона, яку запитують, відповідає на запит шляхом застосування відповідних міжнародних документів, угод і законодавства, на які містяться посилання у статті 23, а також відповідно до інших положень цього розділу.

3. На запит надається термінова відповідь, якщо:

a. існують підстави вважати, що відповідні дані особливо вразливі для втрати або змін; або

b. документи, угоди і законодавство, на які містяться посилання у пункті 2, передбачають термінове співробітництво. Стаття 32 - Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними

Будь-яка Сторона може, не отримуючи дозвіл іншої Сторони:

a. здійснювати доступ до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або

b. здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи.

Стаття 33 - Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу

1. Сторони надають взаємну допомогу одна одній у збиранні даних про рух інформації у реальному масштабі часу, пов'язаних із зазначеною передачею інформації на їх території, яка передається за допомогою комп'ютерної системи. Відповідно до положень пункту 2, ця допомога регулюється умовами і процедурами, які передбачені внутрішньодержавним законодавством.

2. Кожна Сторона надає таку допомогу щонайменше відносно кримінальних правопорушень, стосовно яких проводиться збирання даних про рух інформації у реальному масштабі часу у випадку подібної внутрішньодержавної справи.

Стаття 34 - Взаємна допомога у перехопленні даних змісту інформації

Сторони надають взаємну допомогу одна одній у збиранні або записі у реальному масштабі часу даних змісту інформації у зазначених передачах інформації, які здійснюються за допомогою комп'ютерної системи, у обсягах, які дозволяються відповідними договорами між ними і внутрішньодержавним законодавством.

ВИСНОВКИ

Аналіз, оцінка та використання позитивних здобутків європейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки, адже нині країни стикається з новими викликами та загрозами в інформаційній сфері та перебуває на стадії становлення інформаційного суспільства, яка супроводжується стрімким розвитком інформаційної інфраструктури.

Сьогодні нейтральні країни цілком усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, відтак, питання забезпечення інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях відповідних держав. При цьому політика забезпечення інформаційної безпеки позаблокових країн має проактивний характер і спирається на засади управління ризиками інформаційної безпеки, передусім – кібербезпеки.

Досвід зміни парадигми забезпечення національної безпеки з реактивної на проактивну у контексті євроінтеграційних спрямувань є надзвичайно важливим, адже дозволяє правильно визначати стратегічні пріоритети та оптимізувати зусилля щодо забезпечення інформаційної безпеки, а також сприятиме плідному співробітництву з усіма європейськими країнами у розбудові систем регіональної та міжнародної інформаційної безпеки. Не менш важливим є цей досвід і для подальшої розбудови теорії національної безпеки та наукових засад забезпечення інформаційної безпеки. Зокрема, до перспективних напрямів подальшого наукового пошуку належить передусім дослідження у сфері оцінювання загроз інформаційній безпеці та методів управління ризиками в інформаційній сфері.

На міжнародному рівні занепокоєння державних суб’єктів викликають спроби встановити контроль над глобальним інформаційним простором за допомогою ІКТ. При цьому особливої ваги набуває питання поваги до прав людини й забезпечення основних свобод в інформаційній сфері. Водночас дотримання цих прав і свобод не має суперечити двом найважливішим принципам міжнародного права - невтручання у внутрішні справи держав і поваги до національного суверенітету.

У теперішній час одним із ключових чинників державної політики України чітко визначено вступ до НАТО. З метою набуття членства в Альянсі Україна активізує зусилля з усього комплексу реформ, у тому числі у безпековому та оборонному секторах. Ураховуючи, що саме інформаційна безпека є наразі одним із найважливіших аспектів забезпечення національної, регіональної та міжнародної безпеки в цілому, наша країна має запровадити достатньо заходів перестороги та процедур для її гарантування відповідно до положень політики НАТО у цій сфері, а також дотримати умов, зафіксованих у плані дій Україна – НАТО. Це, зокрема, передбачає:

• забезпечення реалізації гарантій доступу до інформації;

• імплементацію відповідного законодавства для усунення перешкод діяльності ЗМІ;

• поглиблення інформаційного виміру співпраці Україна-НАТО, включаючи парламентське співробітництво;

• створення прозорої та гнучкої структури електронного урядування;

• забезпечення розвитку спроможностей військових частин і підрозділів інформаційних операцій;

• підвищення рівня обізнаності громадськості щодо діяльності НАТО;

• підвищення рівня забезпечення інформаційної безпеки, кібербезпеки тощо.

Виходячи з вищевикладеного, можна визначити основні напрями міжнародної діяльності щодо забезпечення міжнародної інформаційної безпеки:

• створення на національному і глобальному рівнях умов для розробки, виробництва і впровадження засобів забезпечення МІБ;

• організація ефективного міжнародного співробітництва у сфері ІКТ;

• спільна боротьба з кіберзлочинністю та інформаційним тероризмом;

• забезпечення захисту ІКТ від шкідливого впливу і зменшення потенційної шкоди від атак на інформаційні системи;

• удосконалення кадрового забезпечення та організаційних заходів, методик навчання фахівців і проведення наукових досліджень у галузі інформаційної та кібербезпеки;

• захист громадської безпеки, державних структур і бізнесу у сфері ІКТ;

• міжнародна діяльність щодо запобігання конфліктам в інформаційному просторі на противагу підходам, які передбачають їх легітимізацію;

• захист інформації та засобів її обробки для успішної реалізації складних сценаріїв на всіх рівнях;

• усебічне дослідження питань використання ІКТ у конфліктах і застосовуваності міжнародного права до дій держав в інформаційному просторі.

Міждержавні домовленості та міжнародне інформаційне право мають бути спрямовані на демілітаризацію міжнародного інформаційного простору. Необхідно доопрацювати й адаптувати механізми міжнародного права щодо сфери інформаційно-комунікаційних технологій, а також створити нові норми, позаяк гонка озброєнь в інформаційному просторі здатна призвести до дестабілізації міжнародної безпеки через порушення наявних домовленостей про роззброєння та в інших сферах.

ПЕРЕЛІК використаних джерел

1. А. Брега. Риск в системе категорий, характеризующих антитезу национальной безопасности. URL: http://www.milpol.ru/data/2009/1- 12/brega\_risk\_ doklad\_ konf\_nb.doc (дата звернення: 27.10.2020)
2. Алексеев С.С. Общая теория права: в 2 т. Т. 1. М.: Юрид. лит., 1981. С. 119.
3. Алексеев С.С. Структура советского права. М.: «Юрид. лит.», 1975. С. 264
4. Амстердамській договір URL:https://www.cvce.eu (дата звернення 15.10.2020).
5. Антипов В. І. Тіньова коміка та економічна злочинність: світові тенденції, українські реалії та правові засоби контролю (теоретико-методологічне узагальнення). Вінниця. 2006 С. 1040
6. Антонов А.Б., Балашов В.Г. Основы обеспечения безопасности личнос¬ти, общества и государства. Москва. 1996. С.36-55
7. Аскин Я. Ф. Философский детерминизм и научное знание. Москва. 1984. С. 188
8. Ачилов И. Л., Лопатин В. Н., Федотов М. А. Информационное право, 2001. С. 789
9. Баранов О. Інститути інформаційного права “Правова інформатика”, № 3 (11) / 2006. С. 39-45
10. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. Вісник Національної академії державного управління при Президентові України. 2014. С. 60-65
11. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України. Систематизація законодавства в Україні: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції. К.: Інститут законодавства Верховної Ради України, 1999. С. 253-255
12. Бондар І.Р. Інформаційна безпека як основа національної безпеки. Mechanism of Economic Regulation. 2014. № 1. С. 68-75
13. Буроменський М. В., Стешенко В. М. та ін. Розробка пропозицій змін і доповнень до законодавчих актів щодо Державної програми адаптації законодавства України до законодавства Європейського Союзу в галузі боротьби зі злочинністю. Питання боротьби зі злочинністю. Харків, 2005. С. 197–200.
14. Вебер М. Избранное. Образ общества : пер. с нем. М. : Юристъ, 1994. С. 704
15. Вус М.А., Нестеров Ю.М. Информационное общество. Информационное право. Информационная безопасность. Актуальные проблемы безопасности информационного пространства. Материалы Всероссийской научно-практической конференции., 1999. С. 19-20
16. Горбулін В. На захист національних інтересів. Політика і час. 1995. № 2. С. 3–8
17. Директива 2005/60/ЄС Європейського Парламенту та Ради про запобігання використанню фінансової системи та фінансування тероризму URL: http://zakon1.rada.gov.ua/cgi-bin/laws /main.cgi?nreg=994\_774. (дата звернення 10.11.2020).
18. Довгань О.Д. Національний інформаційний суверенітет – обʼєкт інформаційної безпеки. Інформація і право. 2014. С.102- 112.
19. Дремин В. Н. Преступность как социальная практика: институциональная теория криминализации общества : монография. Одесса, Юридическая литература. 2009. С. 613.
20. Європейська конвенція про видачу 1957 URL: http://zakon1.rada.gov.ua/laws/show/995\_033 (дата звернення 10.10.2020).
21. Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України» від 08.06.2017 року. URL: www.zakon.rada.gov.ua/laws/show/2091-19 (дата звернення: 10.11.2020).
22. Закон України «Про засади внутрішньої і зовнішньої політики» від 01.07.2010 року. URL: www.zakon.rada.gov.ua/laws/show/2411-17 (дата звернення: 10.11.2020).
23. Закону України «Про Національну поліцію» від 02.07.2015. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/card/580-19 (дата звернення: 13.10.2020)
24. Казаковцев А.В. НАТО и кибербезопасность. Вестн. Волгогр. гос. ун-та. 2012. № 2 С.109-114
25. Конституція України. Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 18.10.2020)
26. Концептуальні засади розвитку системи забезпечення національної безпеки України: аналіт. доп. / О. О. Резнікова, В. Ю. Цюкало, В. О. Паливода, С. В. Дрьомов, С. В. Сьомін. Київ, 2015. С. 58
27. Кресін О. В. Порівняльне правознавство в Україні: сучасна проблематика та перспективи розвитку. *Міжнародне право і національне законодавство*. 2003. С. 58-63.
28. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III (Редакція станом на 14.11.2020)
29. Олійник О. В. Державна політика інформаційної безпекиУкраїни. Юридичний вісник. 2012. №4(25). С.65-69
30. Партнерство заради миру: Рамковий документ, підписаний Україною 8 лютого 1994 року (набув чинності для України 8 лютого 1994 року). *Офіційний вісник України*. 2006. С. 3232
31. План дій Україна-НАТО (за матеріалами Національного центру з питань Євроатлантичної інтеграції України. URL: http://www.nceai.gov.ua/plan.phtml (дата звернення: 10.10.2020).
32. Політанський В.С. Інформаційне суспільство в Україні: від зародження до сьогодення. Науковий вісник Ужгородського національного університету: серія «Право». 2017. С.16-22
33. Постанова Пленуму Верховного Суду України від 3 берез. 2000 р. № 3. URL: ttp://zakon5.rada.gov.ua/laws/show/v0003700-00. (дата звернення: 15.10.2020)
34. Про Кабінет Міністрів України : Закон України від 27.02.2014 р. № 794-VII. Відомості Верховної Ради України. 2014. № 13. Ст. 222.
35. Про Національний банк України: Закон від 25 травня 1999 р. № 679- XIV. Відомості Верховної Ради України. 1999. № 29. Ст. 238.
36. Про оборону України: Закон України від 06.12.1991 р. № 1932-XII. Верховної Ради України. 1992. № 9. Ст. 106.
37. Про прокуратуру: Закон України від 14.10.2014 р. № 1697-VII. Відомості Верховної Ради України. 2015. № 2-3. Ст. 12.
38. Про центральні органи виконавчої влади: Закон України від 17.03.2011 р. № 3166-VI. Відомості Верховної Ради України. 2011. № 38. Ст. 385.
39. Проблеми застосування в Україні норм інформаційної безпеки НАТО. URL: http://www.db.niss.gov.ua/docs/polmil/1fgs93.htm (дата звернення: 10.10.2020).
40. Радовий Д. О. Проблеми інформаційної політики України на сучасному етапі. *Проблеми теорії і практики*. Київ, 2009. С. 12–16.
41. Рішення Ради ЄС 2007/854/JNA системи Національних агентств з повернення активів (ARO). 2002 URL: http://eur-lex.europa.eu (дата звернення: 02.10.2020.).
42. Салтевський М. В. Інформаційна безпека (у сучасному викладі): *Підручник*. Київ, 2006. С. 588.
43. Скалацький В. М. Концептуальні побудови та практичні моделі інформаційного суспільства. *Гуманітарний часопис*. Харків, 2012. № 4. С. 62-69.
44. Ткачук Т. Ю. Субʼєкти забезпечення інформаційної безпеки держави: функціональний аналіз. Jurnalul juridic national: teorie şi practică. 2017. С. 42–46
45. Ткачук Т. Ю. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства : мат. наук.-практ. конф. Київ. 2017. С. 111–114
46. Угода між Україною та Європейським поліцейським офісом про стратегічне співробітництво. URL: http://zakon1.rada.gov.ua/cgi-bin/ laws/main.cgi?nreg =994\_954. (дата звернення: 08.10.2020.).
47. Указ Президента України «Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2017 рік» від 08.04.2017 № 103/2017. URL: http://www.president.gov.ua/documents/1032017-21670 (дата звернення: 10.10.2020).
48. ФГВФО. Звіт за 2012 р. URL:http://www.fg.gov.ua/files/ docs/reports/Zvit\_FGVFO\_ukr\_2012.pdf. (дата звернення: 12.10.2020.)
49. Феденько С. Взаємодія України з НАТО у сфері інформаційної безпеки. URL: http://nato.pu.if.ua/old/ jornal/2009/2009-35.pdf (дата звернення: 22.10.2020).
50. Фріс, П. Л. Кримінально-правова політика Української держави: теоретичні, історичні та правові проблеми. *Монографія*. Київ, 2005 С. .544.
51. Фріс, П. Л. Нарис історії кримінально-правової політики України: монографія. Київ, 2005. С. 41–57.
52. Хавронюк М. І. Кримінально-правова система в Україні у взаємодії із зарубіжними кримінально-правовими системами (частина І) Вісник Асоціації кримінального права України : електронне наукове видання. 2015. С. 18–70. URL: http://nauka.nlu.edu.ua /wpcontent/uploads/2015/07/4\_2.pdf. (дата звернення: 12.10.2020.)
53. Центр информационной безопасности НАТО выпустил книгу о кибервойне Украины с Россией. URL: http://www.dut.edu.ua/ru/news-1-574-2267 (дата звернення: 15.10.2020).
54. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. Відомості Верховної Ради України. 2003. №№ 40-44. Ст.356.
55. Шертук В. М. Хакерська атака. Правова кваліфікація. *Науковий вісник*. Чернівці, 2017. С. 134.
56. Шушкевич С.В. Протидія інформаційній війні Матері*али міжнародної науково-практичної конференції*. Одеса, 2012. С. 499–502.
57. Al. S. Roberts. Entangling Alliances: Nato’s security of information policy and the entrenchment of State Secrecy. URL: https://www.researchgate.net/profile/Alasdair\_Roberts/publication/228222455 (дата звернення: 10.10.2020).
58. Background information on the Alliance, its policies, activities and structures. URL: http://www.nato.int/cps/en/natohq/topics.htm (дата звернення: 22.10.2020).
59. Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO). URL: www.statewatch.org/news/2006/sep/nato-secclassifications.pdf (дата звернення: 22.10.2020).
60. Hughes, R.B. NATO and Cyber Security: Mission accomplished? URL: http://www.carlisle.army.mil/DIME/documents/ NATO%20and%20Cyber%20Defence.pdf (дата звернення: 15.10.2020).
61. John E Dunn. NATO clause V could deter cyber attack, says defence minister. URL: https://www.networkworld.com/ article/2194246 (дата звернення: 10.10.2020).
62. Kaija E. Schilde. Cosmic top secret Europe? The legacy of North Atlantic Treaty Organization and cold war US policy on European Union information policy. URL: http://dx.doi.org/10.1080/09662839.2014.911175 (дата звернення: 22.10.2020).
63. Kempf, A. Considerations for NATO Strategy on Collective Cyber Defense URL: http://csis.org/blog/considerations-nato-strategy-collectivecyberdefense (дата звернення: 26.10.2020).
64. NATO CCD CoE General Trends: [Online tool]. – Available at URL: http: //www.ccdcoe.org/8.html (дата звернення: 15.10.2020).
65. NATO CCD CoE Mission and Vision. URL: http: //www.ccdcoe.org/11.html (дата звернення: 10.10.2020).
66. NATO Cyber defence. URL: http://www.nato.int/cps/en/natohq/topics\_78170.htm (дата звернення: 15.10.2020).
67. NATO Warsaw Summit Communiqué, 9 July 2016 URL: http://www.nato.int/cps/en/natohq/official\_texts\_133169.htm (дата звернення: 15.10.2020).
68. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. URL: http://www.nato.int/ lisbon2010/strategic–concept–2010–eng.pdf (дата звернення: 10.10.2020).
69. North Atlantic Treaty Organization. Defending against cyber attacks. URL: http://www.nato.int/cps/en/natolive/topics\_49193.htm (дата звернення: 10.10.2020).
70. The North Atlantic Treaty. Washington D.C. URL: www.nato.int/cps/ru/natohq/official\_text\_17120.htm (дата звернення: 18.10.2020)
71. William D. Gerhard, Henry W. Millington Attack on a Sigint Collector.URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa10.pdf (дата звернення: 22.10.2020).