**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 запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

Виконав: слухач магістратури, групи \_8.2629-1

спеціальності

262 Правоохоронна діяльність \_\_\_\_

(шифр і назва спеціальності)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Д. Власов \_\_\_\_\_\_\_\_\_\_\_\_

(ініціали та прізвище)

Керівник доц. каф., доц., к.ю.н. Самойленко Г.В.

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

Рецензент доц. каф., доцент, к.ю.н. Ткалич М.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 Студенту

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Власову Артуру Дмитровичу \_\_\_\_\_\_\_\_\_\_\_\_

(прізвище, ім’я, по батькові)

1. Тема роботи (проекту) Міжнародно-правові стандарти запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

керівник роботи \_\_\_\_ Самойленко Георгій Валерійович, к.ю.н., доцент\_\_\_\_,

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

затверджені наказом ЗНУ від «\_\_\_\_»\_ 2020 року №\_\_ \_\_\_\_\_

1. Строк подання роботи \_\_\_02 листопада 2020 р. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Вихідні дані до роботи \_\_нормативно-правові акти, доктринальні джерела, статті, підручники, статистична інформація\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) стан злочинності у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку; види злочинів у цій сфері; нормативне регулювання запобігання кіберзлочинам; міжнародно-правове регулювання правовідносин у сфері запобігання та боротьби з кіберзлочинами; зміст міжнародних стандартів з запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку; основні проблеми протидії злочинам у цій сфері; кіберзагрози національній безпеці України та запобігання їм

5 Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Консультанти розділів роботи

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  консультанта | Підпис, дата | |
| завдання  видав | завдання  прийняв |
| 1 | Самойленко Г.В., доцент |  |  |
| 2 | Самойленко Г.В., доцент |  |  |
|  |  |  |  |
|  |  |  |  |

1. Дата видачі завдання\_\_\_\_\_травень 2020 р.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №  з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
| 1 | Обрання та затвердження теми | лютий 2020 | виконано |
| 2 | Розробка та узгодження плану | березень 2020 | виконано |
| 3 | Робота з джерелами | квітень 2020 | виконано |
| 4 | Написання пояснювальної записки | травень-червень 2020 | виконано |
| 5 | Написання практичної частини | липень 2020 | виконано |
| 6 | Формування висновків | липень-серпень 2020 | виконано |
| 7 | Оформлення списку використаних джерел | вересень 2020 | виконано |
| 8 | Публікація тез | травень- жовтень 2020 | виконано |
| 9 | Попередній захист на кафедрі | листопад 2020 | виконано |
| 10 | Проходження нормоконтролю | листопад 2020 | виконано |
| 11 | Захист роботи | грудень 2020 | виконано |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Слухач \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_ А.Д. Власов \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

Керівник роботи (проекту) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_Г.В. Самойленко\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

**Нормоконтроль пройдено**

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_М.В. Титаренко\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Власов А.Д. Міжнародно-правові стандарти запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Запоріжжя, 2020. 136 с.

Кваліфікаційна робота складається зі 136 сторінок, містить 110 джерел використаної інформації.

Зі збільшенням опори на цифрові технології, стає все більш важливим питання захисту всіх аспектів Інтернет-інформації та даних. У міру зростання Інтернету, збільшення комп’ютерних мереж, поширення через мобільного інтернету 4G та 5G, тотальної діджіталізації, використання компютерних та інших цифрових технологій практично у всі сфери людського буття, потреба забезпечення безпеки та конфіденціальності інформації та доступу до цифрових (компютерних) пристроїв за допомогою телекомунікаційних мереж набуває все більшого значення. Це значення зростає пропорційно зростанню злочинів, які вчиняються у сфері використання електронних обчислювальних машин (комп’ютерів), систем, електроних мереж та мележ електрозв’язку. У світі ці злочини отримали назву кіберзлочинів.

Федеральне бюро розслідувань США та Інститут комп'ютерної безпеки в ході опитування компаній, що належать до списку Fortune 500, виявили, що вже в період з 1997 по 1999 рік фінансові збитки від комп'ютерних злочинів перевищили 360 мільйонів доларів. На сьогоднішній день ця цифра в рази більша. Злочинці, які здійснюють кіберзлочини отриали найменування «хакери».

На сьогоднішній день Інтернет-шахрайство, віруси та пов'язані з ними деструктивні програми, порушення авторських прав, крадіжка послуг та даних та пов'язані з ними правопорушення вже щорічно приносять збитки на мільярди доларів.

Самі ж злочини в мережі Інтернет схожі на давно встановлені злочини: крадіжки, шахрайство, вандалізм, проступки, переслідування, дитяча порнографія та порушення авторських прав. Майже всі вони здійснюються в Інтернеті, який забезпечує високу ступінь анонімності злочинців, а також потенційний доступ до персональних, ділових та державних даних. Багато комп’ютерних злочинів вчиняються як засіб викрадення грошей або цінної інформації, хоча фінансова вигода не завжди є метою. Наразі забезпечення безпеки інформаційних систем є міжнародною справою, оскільки самі інформаційні системи часто перетинають національні межі, і проблеми, які вони породжують, можуть бути найбільш ефективно вирішені за допомогою міжнародних консультацій та співпраці.

Об’єктом дослідження даної кваліфікаційної роботи є суспільні відносини в сфері запобігання комп’ютерним злочинам.

Предметом дослідження є міжнародно-правові стандарти запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Тому метою кваліфікаційної роботи є встановлення міжнародно-правових стандартів запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку та визначення особливостей їх застосування в Україні.

Теоретико-методологічною основою дослідження є концептуальні положення, визначені міжнародними стандартами запобігання кіберзлочинам. В процесі дослідження було використано діалектичний, порівняльно-правовий, догматичний методи наукового пізнання, а також аналізу та синтезу.

Комп’ютер, інтернет, мережа, кіберзлочин, комп’ютерний злочин, крадіжка, злом, шахрайство, кібертероризм, запобігання, протидія

SUMMARY

Vlasov A.D. International legal standards for the prevention of crime in the use of computers (computer) systems and computer networks and telecommunications. Zaporizhzhia, 2020. 136 p.

The qualification work consists of 136 pages, contains 110 sources of information used.

With increasing reliance on digital technology, the protection of all aspects of Internet information and data is becoming increasingly important. As the Internet grows, computer networks expand, 4G and 5G mobile Internet spread, total digitalization, use of computer and other digital technologies in almost all spheres of human life, the need to ensure security and confidentiality of information and access to digital (computer) devices through telecommunications networks is becoming increasingly important. This value increases in proportion to the increase in crimes committed in the use of electronic computers, systems, electronic networks and telecommunication networks. In the world, these crimes are called cybercrimes.

The US Federal Bureau of Investigation and the Institute for Computer Security in a survey of Fortune 500 companies found that between 1997 and 1999, the financial damage from computer crimes exceeded $ 360 million. To date, this figure is many times higher. Criminals who commit cybercrime are called "hackers".

Today, Internet fraud, viruses and related destructive programs, copyright infringement, theft of services and data, and related offenses already cause billions of dollars in damage each year.

The crimes themselves on the Internet are similar to long-established crimes: theft, fraud, vandalism, misdemeanors, harassment, child pornography and copyright infringement. Almost all of them are carried out on the Internet, which provides a high degree of anonymity for criminals, as well as potential access to personal, business and government data. Many computer crimes are committed as a means of stealing money or valuable information, although financial gain is not always the goal. At present, the security of information systems is an international affair, as the information systems themselves often cross national borders, and the problems they create can be most effectively addressed through international consultation and cooperation.

The object of study of this qualification work is public relations in the field of prevention of computer crimes.

The subject of the study is international legal standards for crime prevention in the use of computers, systems and computer networks and telecommunications networks.

Therefore, the purpose of the qualification work is to establish international legal standards for the prevention of crimes in the use of electronic computers (computers), systems and computer networks and telecommunications networks and to determine the specifics of their application in Ukraine.

The theoretical and methodological basis of the study are the conceptual provisions defined by international standards for the prevention of cybercrime. In the course of the research dialectical, comparative-legal, dogmatic methods of scientific cognition, as well as analysis and synthesis were used.

COMPUTER, INTERNET, NETWORK, CYBER CRIME, COMPUTER CRIME, THEFT, BREAKING, SCAM, CYBERTERRORISM, PREVENTION, COUNTERFEIT

ЗМІСТ

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

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

РОЗДІЛ 2. ПРАКТИЧНА ЧАСТИНА…………………………………………..41

2.1 Стан злочинності у сфері використання електронно-

обчислювальних машин (комп’ютерів), систем та комп’ютерних

мереж і мереж електрозв’язку....................................................................41

2.2 Види злочинів у сфері використання електронно-обчислювальних

машин (комп’ютерів), систем та комп’ютерних мереж і мереж

електрозв’язку …………………………………………………………….44

2.3 Нормативне регулювання запобігання злочинам у сфері

використання електронно-обчислювальних машин (комп’ютерів),

систем та комп’ютерних мереж і мереж електрозв’язку.…….................63

2.4 Міжнародні акти, що закріплюють стандарти запобігання злочинам

у сфері використання електронно-обчислювальних машин

(комп’ютерів), систем та комп’ютерних мереж і мереж

електрозв’язку………………………………………………….…………74

2.5 Зміст міжнародних стандартів з запобігання злочинам у сфері

використання електронно-обчислювальних машин (комп’ютерів),

систем та комп’ютерних мереж і мереж електрозв’язку………………..96

2.6 Основні проблеми протидії злочинам у сфері використання

електронно-обчислювальних машин (комп’ютерів), систем та

комп’ютерних мереж і мереж електрозв’язку………………………….109

2.7 Кіберзагрози національній безпеці України та запобігання їм……110

ВИСНОВКИ………….........................................................................................118

ПЕРЕЛІК використаних джерел…………….......................................124

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРУ Верховна Рада України

ВСУ Верховний Суд України

КМУ Кабінет Міністрів України

п. пункт

р. рік

ст. стаття

ст. століття

РОЗДІЛ 1 ПОЯСНЮВАЛЬНА ЗАПИСКА

*Актуальність теми.* Мережа комп’ютерів, що охоплює земну кулю, дозволяє людям практично в будь-якій країні чи штаті вчиняти протиправні дії в будь-якому іншому місці, якщо в обох місцях є комп’ютер та Інтернет. Велике охоплення, відносна анонімність Інтернету, особливо при використанні динамічних адрес, ускладнює працівникам правоохоронних органів відстежити суб’єкта злочинної діяльності через її джерело (точку входу чи IP адресу, яку вправні хакери маскують через удовження та зміну маршрутизатора).

Насправді, деякі найвідоміші випадки комп’ютерних злочинів здійснювалися хакерами, які прагнуть «похвалитися правами», долаючи заходи урядової та корпоративної безпеки.

Загалом, інтернет та комп’ютерні мережі та засоби є лише способом здійснення злочинів, відомих Кримінальному кодексу: крадіжка, шахрайство, вимагання викупута тероризм. Проте, окремі дії полягають не стільки у заволодінні фінансовими ресурсами, скільки у завданні шкоди внаслідок втручання в роботу коп’ютерних мереж та мереж електрозв’язку, паралізуючи тим самим діяльність не лише приватного сектору, але і державних установ, медичних закладів, тощо. В залежності в масштабу, наслідків та замовлень, суб’єктів, яким це вигідно, інколи виступають не лише окремі громадяни, але і спецслужби (в т.ч. розвідка, контррозвідка іноземних держав). В останньому випадку може йтися про необ’явлену війну економічного характеру, або одного із проявів гібридної війни.

Тому тут існує проблема подвійного характеру: 1) вчинення злочину; 2) вчинення злочину шляхом використання середовища його вчиненяння: мережі Інтернет чи інших компютерних мереж чи мереж телекомунікацій. Тому ці злочини обумовлені, здебільшого, природою Інтернету.

Для запобігання тому вже зроблено чимало: це антивірусні програми, «пісочниці безпеки», формування відділів запобігання компютерним злочинам та несанкціонованого втручання в роботу мереж, систем, серверів, комп’ютерних програм, функціонування інших електронно-обчислювальних машин та пристроїв, включаючи смартфони, планшети та ін., які використовують платформу для комунікацій на основі мережі Інтернет, формування відділів боротьби в органах національної поліції та Служби безпеки України (кіберполіція).

Проблема скоєння комп’ютерних злочинів (кіберзлочинів) полягає в: 1) середовищі скоєння; 2) застосованих засобів скоєння (як правило, це використання спеціалізованих програм, включаючи програми типу «троянський кінь», кодів та ін.); 3) транснаціональний характер (а фактично, відсутність кордонів) чи екстериторіальний характер; 4) рівень підготовки та кваліфікації злочинців (як правило, талановитих та обдарованих та високопідготовлених професіоналів-програмістів); 5) специфічність суб’єкта скоєння злочину (особи, що спеціалізується на комп’ютерному програмуванні, якщо не брати до уваги організовану злочинність, де як правило, така особа є фактичним виконавцем такого злочину).

На міжнародному рівні, рівні ЄС та окремих країн застосовуються заходи, орієнтовані на: 1) запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку; 2) протидію їм; 3) боротьбу з ними (тут, здебільшого, йдеться про притягнення до відповідальності злочинців).

Слід визнати, що компютерні мережі та технології скорочують час та простір. Багато процесів стають доступними та автоматизованими, чому сприяла мінітюаризація процесів, особливо в сфері мобільного зв’язку та мобільного інтернету. Зросла комп’ютерна грамотність. Водночас, така тотальність має і зворотню сторону, - уразливість. Ця уразливість дозволяє злочинцям діяти. Застосування засобів захисту зумовлює витонченість, грамотність та навіть креативність злочинців, адже йдеться про спосіб порівняно легко дістатися до фінансів та грошей.

До того ж, комп’ютерні системи мають порівняно нові, але надзвичайно складні можливості для порушення законодавства, що створює потенціал для вчинення традиційних видів злочинів нетрадиційними способами.

Та окреім доступу економічної злочинності до чужих коштів, зокрема. Коштів, які зберігаються на банківських рахунках, суспільство визнало зручним спосіб комунікації та автоматизацції процесів, в т.ч. укладання електронних правочинів, а тому в буденному житті покладається на комп’ютеризовані системи, починаючи від контролю за повітряним, залізничним та автобусним рухом, закінчуючи координацією медичних служб та національної безпеки. Навіть невеликий збій у роботі цих систем загрожує життю людей. Відтак, суспільство, економіка та окремо взята людина стає залежною від функціонування комп’ютерних систем та засобів зв’язку.

Швидке транснаціональне розширення широкомасштабних комп’ютерних мереж та можливість доступу до багатьох систем через звичайні телефонні лінії, як лінії електрозвязку, так і мобільний зв'язок, збільшує вразливість цих систем та можливість зловживання чи навіть злочинної діяльності. Наслідки комп'ютерної злочинності можуть мати як серйозні економічні витрати, так і серйозні втрати з точки зору безпеки людини.

Проблема запобігання та протидії кіберзлочинам має різні вектори та площини. Основною з них є міжнародна проблема. Справа в тому, що комп’ютерні технології розвиваються надшвидкими темпами, а системи кримінального правосуддя та міжнародне співробітництво не йдуть в ногу з технологічними змінами. Лише декілька країн мають адекватні закони для вирішення проблеми, і з них жодна не вирішила всіх юридичних, правозастосовчих та запобіжних проблем.

В Україні ця проблема частково вирішена шляхом значного оновлення Кримінального кодексу України, внесення до нього Розділу XVI (Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку). Статтями цього Розділу передбачено окремі склади злочинів. Криміналізація протиправних дій в сфері функціонування комп’ютерних мереж та мереж електрозв’язку свідчить про негативну реакцію суспільства та держави до таких дій та їх суспільну небезпечність.

В такому випадку, коли Кримінальний кодекс урахував небезпечність окремих видів діянь і конкретизував їх, зокрема: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку(ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 3611 КК України); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України); порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України).

Де-факто, криміналізація цих діянь виходить далеко за рамки крадіжки грошей з банківських рахунків фізичних та юридичних осіб за допомогою компютерних технологій через системи «клієнт-банк» та внутрішньобанківські компютерні мережі, чи навіть шляхом втручання в роботу платіжно-розрахункової системи Національного Банку України.

Українській банківській системі відома і справа, яка розслідувалася свого часу СБУ України, коли злочинна організація, використовуючи спеціальне обладнанння та програмне забезпечення, перехоплювала інформаційні платіжні файли (пакети), які проводили в пізній операційний час, використовувала їх у якості платіжних ресурсів за кордоном (переважно США, де в нічний український час був день, а відповідно, і банківська ділова активність). Після використання фінансових ресурсів вночі, зранку про-файли поверталися на місце. Тож, фактично, збитки а ні банківській системі, а ні НБУ, а ні окремим фізиним чи юридичним особам не завдавалося. Фактично, був відсутній склад злочину «крадіжка». Але мало місце несанкціоноване втручання в роботу банківської системи, і НБУ, зокрема, що мало високу ступінь ймовірності завдання шкоди не лише їм, але й національній безпеці України взагалі.

На перший погляд і таке діяння, як створення і розповсюдження вірусних програм, може викликати заперечення щодо визнання його злочином, адже лише його використання може завдати шкоди як прямої, так і опосередкованої, коли, скажімо, множення файлу вичерпує операційну пам'ять комп’ютера і фатально обмежує здатність ЕОМ робити обчислення чи виконувати певні операції, що спричиняє затримку, а інколи і збій в роботі не лише коремих компютерів, підприємств чи організацій, але й окремих сфер економіки. Чого вартий збій автоматизованих систем управління ПАТ «Укрзалізниця»? не важко уявити.

Зважаючи на серйозність загроз від діянь, якими здійснюється посягання на усталений порядок у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, доступність для транснаціональних посягань, гіперактивний ступінь розвитку технологій і «продвинутість» «хакерів», існує потреба в міжнародній співпраці щодо обміну досвідом на «програмному» рівні, організаційному, правовому, діяльнісному та інструментальному (спільна розробка системного та програмного забезпечення, в т.ч. фільтрів «підозрілої» чи «ризикової» активності, взаємне інформування та спільні заходи, в т.ч. на рівні окремого спеціалізованого підрозділу Інтерполу). Міжнародною спільнотою були вироблені окремі заходи запобігання компютерним злочинам (кіберзлочинам), в т.ч. вироблено міжнародні стандарти запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Існує нагальна потреба у їх застосуванні їх як у внутрішному середовищі України, так і в співпраці з іноземними урядовими та міжурядовими організаціями.

Відповідно, метою даного дослідження є встановлення змісту міжнародних стандартів запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, стан та перспективи їх застосування в Україні.

Відповідно до зазначеної мети визначаємо завдання, які потрібно вирішити в цьому дослідженні:

* встановити зміст міжнародних стандартів запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;
* визначити особливості їх застосування в Україні;
* визначити прогалини та недоліки чинного законодавства, які стоять на заваді застосуванню міжнародних стандартів запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку в Україні;
* внести пропозиції щодо удосконалення чинного законодавства та визначення стратегічних напрямків та плану дій з імплементації та застосування міжнародних стандартів запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку в Україні.

*Об’єктом дослідження* даної кваліфікаційної роботи є суспільні відносини в сфері запобігання комп’ютерним злочинам.

*Предметом дослідження* є міжнародно-правові стандарти запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

*Метою* кваліфікаційної роботи є встановлення міжнародно-правових стандартів запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку та визначення особливостей їх застосування в Україні, стан та перспективи їх застосування в Україні.

*Теоретико-методологічною основою* дослідження є концептуальні положення, визначені міжнародними стандартами запобігання кіберзлочинам. В процесі дослідження було використано діалектичний, порівняльно-правовий, догматичний методи наукового пізнання, а також аналізу та синтезу.

### *Ступінь наукової розробки проблеми.* Окремі питання як кримінально- правової характеристики та кваліфікації злочинів у сфері комп’ютерних технологій, так і напрямів протидії їм, були предметом багатьох вчених, зокрема: Азарова Д. С., Антонюк Л., Базилевич В., Біленчука П. Д., Власюк О., Глушкова В. А., Гуторової Н. А., Діхтяренка М.Д., Карчевського Н. В., Кміть В.М., Хавронюк Н. І., Солнцева Н., Селіванова В., Пархомова С., Ляпунова Ю. та зарубіжних науковців: Кемпф В. А., Мініна А. Я., Jim Schonrock, Sean Sands, Ally Marshall, Bridget Molitor, Kit Spielberger та інших.

*Опис проблеми, що досліджується.* Велике значення для боротьби та запобігання діянням, які несуть значну суспільну небезпеку, стало закріплення в КК України Розділу XVI Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Об’єктивно, що окрім крадіжок, існує велика кількість діянь, які здатні причинити шкоду комп’ютерам, комп’ютерним чи мережам електрозв’язку чи їх власникам чи користувачам.

Так, відомий вірус Petya з сімейства шкідливих програм (вражаючих комп'ютери під управлінням сімейства ОС Microsoft Windows, які було виявлено в 2016 році у якості здирницьких вірусів), 27 червня 2017 року був використаний для масштабної атаки, яка полягала в тому, що вірус (програма) був вірусом-винищувачем даних, замаскованим під програму-вимагач. Програма шифрувала файли на жорсткому диску комп'ютера-жертви, а також перезаписувала і шифрувала головний завантажувальний запис (MBR), після чого дані зникали, а операційна система взагалі переставала працювати.

Атака вірусом Petya в 2017 році в Україні завдала істотної шкоди: вірусом були уражені енергетичні компанії, більшість українських банків, аеропортів «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен та ін. Це перша така масова атака, тим більше з такими наслідками: за даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya становили майже 850 млн доларів. Заяви постраждалих компаній до кіберполіції про відшкодування шкоди у звязку з втратою даних залишались незадоволеними через неможливість притягнення злочинця чи злочинців до кримінальної відповідальності через складнощі їх встановлення.

Вважається, що вірус Petya був розроблений та ініційована його атака спецслужбами РФ.

Найменш загрозливим є використання спаму за допомогою комп'ютерів-зомбі, що дозволяє спамерам залишатись інкогніто та знижує їх витрати на розсилку спаму. Але проблема полягає в тому, що спам сприяє поширенню троянських програм, які, на відміну від вірусів, не саморозмножуються. Вони покладаються на рух електронної пошти або збільшення спаму, тоді як хробаки можуть поширюватися за допомогою інших засобів. Тож зомбі можуть використовуватися і для здійснення клікфроду (розмноження рекламних оголошень).

Часто комп'ютери-зомбі утворюють ботнети для розповсюдження спаму електронною поштою і для проведення DoS-атак. Більшість з них орієнтовані на масове звернення до певних серверів, що призводить їх до неможливості реагувати на звернення через їх масовість, що призводить до «зависання» сайту. Може бути вигідно конкурентам. Задля маскування DoS-атаки на цільові сайти роблять через «пульсуючі» зомбі. Відсутність системності атаки ускладнює процес його виявлення (в окремих випадках навіть роками).

Статистичні дані свідчать, що за останні п’ять років в Україні кількість злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку зросла майже в 2,5 разів.

Розвиток інформаційних технологій пропорційно має наслідком зростання злочинності в сфері експлуатації комп’ютерних систем та мереж, мереж електрозв’язку, притому, за останній рік майже вдвічі більше, ніж за аналогічний період минулого року.

Фахівці в сфері ІТ технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. Організована злочинність все частіше використовує Інтернет як засіб вчинення та приховування своєї злочинної діяльності. Злочинна мережа Darknet перетворилася в цифровий чорний ринок для збуту наркотиків, зброї, крадених товарів та ін. За даними Національної поліції України кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилась майже на 36 %.

На сьогоднішній день Управління боротьби з кіберзлочинністю МВС України та СБУ спеціалізовані на бротьбі зі злочинністю в сфері комп’ютерних технологій констатують, що пріоритети та характер кіберзлочинності в Україні змінюються і набувають певних рис, зумовлених змінами в сфері міжнародного запобігання та протидії таким злочинам. Оскільки в провідних зарубіжних країнах посилюються заходи запобігання, протидії та боротьби з комп’ютерними злочинами, нестримно підвищується рівень підготовки кіберфахівців правоохоронних органів та мотивується їх діяльність, українські кіберзлочинці, які раніше вважали «справою честі» «витряхнути кишені західних імперіалістів», то нинішнє покоління кіберзлочинців не має такого «Кодексу честі», а філософія «свободи доступу до цифрового досягнення людства на безкоштовній основі» уходить в минуле. Злочинність в сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку все більше і більше набуває рис звичайної злочинності: цинічної, ганебної, егоїстичної, зверхньої, зневажливої до прав, свобод та інтересів інших людей. Використання низького ступеня обізнаності людей в банківській сфері та цифрових технологіях стало сферою полювання шахраїв, які виманюють персональну інформацію від користувачів дебетових, а то і кредитних карт, і, що найнеприємніше, у і так вкрай збіднілих чи навіть нищих слоїв населення. Йдеться про осіб похилого віку, пенсіонерів.

Україна з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки є для кіберзлочинців та шахраїв «золотою жилою».

Нажаль, розкрадання коштів в системах інтернет банкінгу, даних кредитних карт, DoS атаки на сайти, шахрайство з застосуванням комп’ютерних мереж, несанкціонаовані витоки інформації є вже системним явищем.

За оцінками експертів управління з боротьби з кіберзлочинністю в одному лише Києві чи не щодня фіксуються до двадцяти випадків крадіжки грошей через клієнт-банк. Суми крадіжок становлять від 20.000 грн. до 40.000.000 грн. ЗМі освітлює цю інформацію частково, адже поширення такої інформації не вигідне ні поліції, ні банкам, ні самим потерпілим. Нажаль, певна частина таких злочинів вчиняється ОЗГ, до яких входять співробітники банків та навіть правоохоронних органів.

На сьогоднішній день вже сформовано нормативно-правову базу запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Правову основу інформаційної безпеки України становлять: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України» та ін., Доктрина інформаційної безпеки України, Указ Президента України від 26.05.2015р.№ 287/2015/ «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»», Указ Президента України від 14.03.2016 р. № 92/2016 «Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»», Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов’язковість яких надала Верховна Рада України.

Основними проблемами протидії злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку є: 1) недостатність високопрофесійних фахівців та експертів; 2) недостатній рівень професійної підготовки; 3) затримка проведення комп'ютерно-технічної експертизи до півроку; 4) складнощі з введенням в правове поле досліджень фахівців комерційних організацій; 5) недосконалість Кримінального процесуального кодексу України; 6) перехоплення організованою злочинністю талановитих програмістів з метою вчинення злочинних діянь; 7) обмеженість змістовного наповнення КК України лише злочинами у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку відносно положень Закону України «Про основні засади забезпечення кібербезпеки України», попри реальну прогресивність останнього; 8) відсутність спеціальних норм щодо протидії цим злочинам в КПК України, зокрема, щодо збирання та зберігання електронних доказів, блокування операцій, в т.ч. банківських, накладання арештів; 9) невідповідність норм КПК України щодо накладання арешту відповідно до Постанови слідчого судді потребам терміновості блокування сумнівних цифрових (і в першу чергу, банківських операцій); 10) відсутність нормативної регламентації в КПК України такриміналістичних рекомендацій ефективного виявлення електронних (цифрових) слідів як явища об’єктивної дійсності, їх дослідження, фіксації, вилучення й використання у розслідуванні та попередженні злочинів.

Тому Радою національної безпеки і оборони України визначено, що боротьба з кіберзлочинністю має передбачати здійснення заходів: удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень; врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису; впровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю як на національному, так і міжнародному рівні; запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів; підвищення кваліфікації співробітників правоохоронних органів; підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються кіберзлочинів.

Звертає увагу той факт, що не всі протиправні діяння, які визнані у світі кіберзлочинами, визначені такими в Кримінальному Кодексі України та Законі України «Про основні засади забезпечення кібербезпеки України». Цей закон визначає, що кіберзлочином (комп'ютерним злочином) є суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Але ж, відповідно до Кримінального кодексу України кіберзлочином в Україні визнається лише таке протиправне, суспільно небезпечне діяння, яке визнане у якості такого Кримінальним Кодексом України. Тому виникає справедливе питання, - яким чином кваліфікувати діяння, якщо воно не визнане у якості злочину Кримінальним кодексом України?

Відповідно до Конвенції Ради Європи про кіберзлочинність, ратифікованої Верховною Радою України, імплементованої до українського законодавства з 11.10.2005 р., класифіковано чотири типи кіберзлочинів:

1. правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями;
2. правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами;
3. правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією;
4. правопорушення, пов'язані з порушенням авторських і суміжних прав.

Об’єктивно, що ст. 361-363-1 КК України Розділу XVI (Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку) охоплено лише першу та другу групу.

В світі найпоширенішими видами кіберзлочинів визначено:

* кардинг – шахрайські операції з кредитними картками, не погоджені власником картки (несанкціоновано, без повноважень): крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки. Мета: отримання доступу до чужих грошових коштів. Основний спосіб: фішинг, - використання необізнаності, довірливості та неуважності власника картки;
* Фішинг – шахрайські дії, спрямовані на виманювання реквізитів картки чи /та її рахунку і інформації доступу до нього (логін/пароль) у її власника. Як правило, власник кредитної чи дебетової картки добровільно повідомляє шахраям таку інформацію. Види фішингу:

Аналіз цих видів злочинних діянь дозволяє визначати кіберзлочином дії: втручання в роботу телекомунікаційних мереж, комп’ютерних програм, що функціонують у їх середовищі; несанкціоновану модифікація комп’ютерних даних; дезорганізацію роботи критично важливих елементів інфраструктури держави, що створює небезпеку загибелі людей, завдання значної майнової шкоди або настання інших суспільно небезпечних наслідків.

Найважливішою ознакою таких злочинів є їхній об’єкт посягання. Важаємо, що визначення видів кіберзлочинів має конструювати­ся на основі специфічних ознак їх родового об’єкта. Такий підхід до класифікації за родовим об’єктом як системо­утворюючої основи для побудови норм Особливої частини Кримінального кодексу України.

Окремі науковці наводять наступну класифікацію видів кіберзлочинів і протиправних дій у сфері комп’ютер­ної інформації:

* насильницькі або інші потенційно небезпечні дії, що посягають на фізичну безпеку, життя та здоров’я людини;
* дії, що порушують конфіденційність даних, які містяться чи передаються в інформаційних і телекомунікаційних системах (ці злочини спрямовані на розкриття інформації без зміни її змісту);
* дії, що порушують цілісність даних, їхню доступ­ність для адміністраторів і легальних користувачів (відмо­ва в обслуговуванні), що здатне порушити штатні режими функціонування інформаційних і телекомунікаційних сис­тем різного призначення (злочини, що заподіюють майнові збитки через збій чи зупинку функціонування комп’ютерних систем чи комп’ютерних мереж. Не пов’язані з розкраданням інформації чи грошових коштів);
* дії, що посягають на майно, майнові права, а також на право власності, прав на інформацію чи авторські права;
* дії, що посягають на громадську моральність;
* дії, що посягають на громадську безпеку;
* інші.

Більшість з них належать до традиційних злочинів, які посяга­ють на різні об’єкти, що охороняються законом, але здій­снюються з використанням інформаційних і телекомуніка­ційних систем. Ці злочини можуть бути вчинені без застосування інформаційних і телекому­нікаційних технологій.

В інструктивних матеріалах Інтерполу вживається тер­мін «цифрові злочини» («digital crime»), які поділяються на три групи:

1) комп’ютерні злочини (порушення авторських прав на програмне забезпечення, розкрадання даних, пору­шення роботи обчислювальних та інформаційних комп’ютерних систем, розкрадання комп’ю­терного часу та ін.);

2) злочини, «пов’язані з комп’ютерами» (фінансове шахрайство);

3) мережева злочинність (використання мереж для здійснення незаконних угод, в т.ч. поши­рення порнографії, торгівлі наркотиками, ухилення від митних зборів, відмивання грошей та ін.).

Серед існуючих класифікацій кіберзло­чинів є класифікація, розроблена на основі міжнародної взаємодії в боротьбі з комп’ютерними злочинами та кодифікатора ро­бочої групи Інтерполу, що був покладений в основу автома­тизованої інформаційно-пошукової системи, створеної на початку 90-х рр.

Згідно цього кодифікато­ра, усі кіберзлочини класифіковані:

QA- несанкціонований доступ і перехоплення;

QAH - комп’ютерний абордаж (несанкціонований до­ступ);

QAI - перехоплення за допомогою спеціальних техніч­них засобів;

QAT - крадіжка часу (ухилення від плати за користу­вання);

QAZ - інші види несанкціонованого доступу та пере­хоплення;

QD - зміна комп’ютерних даних;

QDL - логічна бомба;

QDT - троянський кінь;

QDV - комп’ютерний вірус;

QDW - комп’ютерний черв’як;

QDZ - інші види зміни даних;

QF - комп’ютерне шахрайство;

QFC - шахрайство з банкоматами;

QFF - комп’ютерна підробка;

QFG - шахрайство з ігровими автоматами;

QFM - маніпуляції з програмами введення-виведення;

QFP - шахрайства з платіжними засобами;

QFT - телефонне шахрайство;

QFZ - інші комп’ютерні шахрайства;

QR - незаконне копіювання;

QRG - комп’ютерні ігри;

QRS - інше програмне забезпечення;

QRT - топологія напівпровідникових пристроїв;

QRZ - інше незаконне копіювання;

QS - комп’ютерний саботаж;

QSH - з апаратним забезпеченням (порушення роботи ЕОМ);

QSS - із програмним забезпеченням (знищення, блоку­вання інформації);

QSZ - інші види саботажу;

QZ - інші комп’ютерні злочини;

QZB - із використанням комп’ютерних дошок оголо­шень;

QZE - розкрадання інформації, що становить комерцій­ну таємницю;

QZS - передача інформації, що підлягає судовому роз­гляду;

QZZ - інші комп’ютерні злочини.

Цей кодифікатор, який використовує Інтерпол для відправки запитів або повідомлень про комп’ютерні злочини телекомунікаційною мережею, свідчить про достатньо широкий спектр скоюваних в сфері функціонування компютерних пристроїв та компютерних та телекомунікаційних систем, ситем електрозв’язку злочинів.

Інша класифікація кіберзлочинів має критерієм способів втручання до процесу передачі даних: 1) переривання (блоку­вання процесу передачі); 2) перехоплення (неправомірний доступ до передаваних даних); 3) модифікація (неправо­мірна зміна даних); 4) виготовлення (організація сфальси­фікованого сеансу зв’язку).

Інтерполом визначено і інші види злочинів, які входять в коло «кіберзлочинів», зокрема:

1. Cyber Terrorism (кібертероризм) визнаний багатьма країнами та спеціалістами з безпеки інформаційних технологій. Є занепокоєння, що такі вторгнення є частиною організованих зусиль кібертерористів, іноземних спецслужб або інших груп з метою скласти карту потенційних дір в безпеці в критичних системах. Формально, кібертерористом є особа, яка залякує чи примушує уряд чи організацію досягати своїх політичних чи соціальних цілей, здійснюючи комп'ютерну атаку на комп'ютери, мережі чи інформацію, що зберігається на них. Тож кібертероризмом є акт тероризму, що скоєний за допомогою використання кіберпростору або комп’ютерних ресурсів.

Навіть просту пропаганду в Інтернеті про те, що під час свят відбуватимуться бомбові атаки, можна розглядати як кібертероризм. Хакерські заходи можуть бути спрямовані на окремих людей, сім'ї, уряди та країни. Основна мета: викликати страх серед людей, демонструвати владу, здійснювати збір інформації, необхідної для руйнування життя людей, грабежів чи шантажу.

Широкомасштабний вплив на значну кількість людей може послабити економіку країн, позбавляючи їх ресурсів і роблячи її більш вразливою до воєнних нападів. Кібертерор також впливає на бізнес, що базується на Інтернеті. Зупинка роботи інтернет ресурсу підриває економічну стабільність країни та рух коштів. Тим самим впливає і на політичну стабільність країни, а отже, є терором;

1. Заперечення расизму та Голокосту. Расизм, заперечення Голокосту та файли, що містять расистські висловлювання чи публікації, караються, також коли вони розповсюджуються через Інтернет. Сюди входить поняття «cyberhate» (кіберхайту), що стосується виразів ненависті в Інтернеті. Ця ненависть відображається на расизмі: використанні знущань (залякування в Інтернеті), образ або насильства на основі будь якої дискримінаційної ознаки. Дискримінація за ознакою статі, сексуальної орієнтації, релігії чи життєвої філософії також підпадає під поняття «кіберхайта», як і висловлення ненавісті антисемітизму та запереченням Голокосту: заперечення, мінімізація, виправдання або схвалення геноциду, скоєного під час Другої світової війни;
2. Cyberextortion - Кіберекстрація - злочин, пов’язаний з нападом або загрозою нападу у поєднанні з попитом. В Інтернет-сленгу «троль» - це людина, яка сіє розбрат в Інтернеті, висловлюючи суперечки або засмучуючи людей, публікуючи запальні, сторонні повідомлення або повідомлення, що не стосуються теми. Інтернет-спільнота, наприклад група новин, форум, чат або блог з навмисним наміром викликати читачів на емоційний відгук або іншим чином порушити нормальну дискусію на тему, часто для власної розваги, за гроші, щоб запобігти або зупинити атаку.

Окремою формою тролінгу є різні форми вимагання. Спочатку напади відмови в обслуговуванні (DoS) на корпоративні веб-сайти є найпоширенішим методом кіберектори. Зловмисник може ініціювати пінг-шторм і зателефонувати президенту компанії, вимагаючи внести гроші на банківський рахунок в іноземній країні в обмін на припинення нападу.

Наразі цей вид змінено на застосування програм-вимагачів, які шифрують дані жертви. Жертва отримує електронне повідомлення, яке пропонує приватний ключ розшифровки в обмін на грошовий платіж у біткойнах. На жаль, як і при інших видах вимагання, оплата не гарантує, що подальші кібератаки не будуть розпочаті. Більшість зусиль, пов’язаних з кібератарством, ініціюються через зловмисне програмне забезпечення у вкладеннях електронної пошти або на скомпрометованих веб-сайтах;

1. Cyberbullying - Кібер-знущання. Кібер-залякування визначається в юридичних глосаріях як:

- дії, що використовують інформаційно-комунікаційні технології для підтримки навмисної, повторюваної та ворожої поведінки окремої особи чи групи, яка має на меті завдати шкоди іншій особі чи іншим особам;

- використання комунікаційних технологій з метою заподіяння шкоди іншій особі чи іншим особам;

- використання Інтернет-послуг та мобільних технологій, таких як веб-сторінки та дискусійні групи, а також обмін миттєвими повідомленнями або SMS-повідомленнями з метою заподіяння шкоди іншій особі чи іншим особам.

Кібер-залякування можна розглядати як відмінність від інших форм поведінки в Інтернеті. Інколи кібер-знущання розуміють як форму кіберсталінгу, що передбачає більш стратегічний підхід, ніж інтернет-тролінг.

Згідно з Конвенцією Ради Європи по боротьбі з кіберзлочинністю, виділяється чотири основні типи кіберзлочинів:

1. Злочини проти конфіденційності, цілісності та до­ступності комп’ютерних даних і систем:

* несанкціонований доступ до інформаційного середо­вища, здійснений шляхом протиправного навмисного доступу до комп’ютерної системи або її частини, вченений в обхід систем безпеки;
* незаконне перехоплення – протиправне нав­мисне перехоплення не призначених для загального досту­пу комп’ютерних даних, які передаються комп’ютерними системами, яке здійснюється шляхом використання технічних засобів в обхід заходів безпеки;
* втручання в дані - протиправна зміна, пошкодження, ви­далення, спотворення або блокування комп’ютерних даних;
* втручання в роботу системи - протиправне порушен­ня або створення перешкод функціонуванню комп’ютерної системи;
* незаконне використання комп’ютерного і телекому­нікаційного устаткування - виготовлення, придбання для використання, поширення або надання доступу: а) пристроїв та комп’ютерних програм, розроблених або пристосованих для здійснення зло­чинів; б) комп’ютерних паролів, кодів доступу, інших даних, які забезпечують доступ до комп’ютерної систе­ми або її частини за наявності наміру використання їх з метою здійснення будь-якого із зазначених вище злочинів; володіння одним із перелічених предметів із наміром використати його для здійснення будь-якого зі злочинів.

1. Шахрайство та підробка, що пов’язані з використан­ням комп’ютерів:

* підробка документів із застосуванням комп’ютерних засобів - протиправне умисне внесення, зміна, видалення або блокування комп’ютерних даних, що призводить до зниження їхньої достовірності, припускає, що згодом вони розглядатимуться як достовірні;
* шахрайство із застосуванням комп’ютерних засобів - втручання у функціонування комп’ютерної системи з об­манним або нечесним наміром умисного протиправного отримання економічної вигоди для себе або для інших осіб.

1. Злочини, пов’язані з розміщенням у мережах проти­правної інформації:

* злочини, пов’язані з дитячою порнографією, - по­ширення дитячої порнографії за допомогою глобальних мереж, пропозиція або надання доступу до неї, отримання для себе або інших осіб за допомогою комп’ютерної сис­теми, зберігання дитячої порнографії в комп’ютерній сис­темі.

1. Злочини щодо авторських і суміжних прав, які здійснюються шляхом викорис­танням комп’ютерної системи злочини щодо прав, передбачених низкою відповідних міжнародних актів щодо захисту авторських та суміжних прав та інших об’єктів права інтелектуальної власності.

Комітетом який розробляв проект Конвенції по боротьбі з кіберзлочинністю, обговорювалася можливість включення до типології й інших порушень, пов’язаних із використан­ням глобальних мереж, зокрема, пропаганда расизму в Інтернеті. Проте, згода з цього питання учасниками Ради Європи не була досягнута.

Усвідомлюючи транснаціональний характер кіберзлочинів в силу транснаціонального характеру функціонування глобальної мережі Інтернет, свого часу виникло питання міжнародного співробітництва у сфері протидії комп’ютерним злочинам.

В 1983 р. Організація економічного співробітництва та розвитку (ОЕСР) провела дослідження можливості міжнародного застосування та гармонізації кримінального законодавства для вирішення проблеми комп’ютерних злочинів або зловживань. У 1986 р. ОЕСР опублікував звіт «Комп'ютерна злочинність: аналіз правової політики». В ньому було проведено дослідження існуючих законів та пропозицій щодо реформ у ряді держав-членів та рекомендовано мінімальний перелік зловживань, які країни повинні розглянути, забороняючи та караючи кримінальним законодавством, наприклад, комп'ютерне шахрайство та підробка, зміна комп'ютерних програм та даних, порушення авторських та суміжних прав, перехоплення засобів зв'язку або інших функцій комп'ютера або телекомунікаційних систем.

Члени Комітету з питань інформації, комп’ютерів та політики зв’язку рекомендували запровадити кримінальну відповідальність захист щодо інших видів протиправних дій, зокрема, крадіжку комерційної таємниці та несанкціонований доступ до комп’ютерних систем або їх використання.

Після Звіту ОЕСР, Рада Європи розпочала власне дослідження цього питання з метою розробки керівних принципів, які допоможуть законодавцям у визначенні того, яка поведінка повинна бути заборонена кримінальним законодавством і як цього слід досягти, зважаючи на конфлікт інтересів між громадянськими свободами та необхідністю їх захисту в мережі Інтернет.

Мінімальний перелік злочинних дій в компютерному середовищі, який було розроблено ОЕСР був значно розширений.

Комісією експертів з комп'ютерної злочинності Комітету з проблем злочинності було розширено сферу і включено: захист приватного життя жертви, запобігання, процедурні питання, такі як міжнародний пошук та вилучення банків даних, а також міжнародне співробітництво у розслідуванні та переслідування комп'ютерних злочинів. Рекомендація R(89)9 Ради Європи щодо злочинів, пов'язаних з комп'ютером, яка містить керівні принципи для національних законодавчих органів, була прийнята Комітетом міністрів Ради Європи 13 вересня 1989 року.

В 1992 р. ОЕСР розробила набір керівних принципів щодо безпеки інформаційних систем, який покликаний забезпечити основу, на якій держави та приватний сектор можуть створити основу для безпеки інформаційних систем. Того ж року Рада Європи розпочала дослідження, яке зосередиться на процедурних та міжнародних питаннях співпраці, пов'язаних із комп'ютерною злочинністю та інформаційними технологіями.

Необхідність глобальних дій.

Незважаючи на ці міжнародні зусилля, для досягнення міжнародної співпраці ще багато чого потрібно зробити. На сьогоднішній день забезпечення цілісності комп’ютерних систем є викликом для сучасної міжнародної економіки. Тому на всіх рівнях (приватноу, місцевому, міжнародному, регіональному, державному, міжнародному) все більше уваги приділяється кібербезпеці. Не виключенням стала і Україна, яка прийняла низку актів, спрямовану на забезпечення кібербезпеки на рівні національної безпеки України.

Участь практично всіх країн світу в міжнародних ініціативах щодо комп’ютерних злочинів є обнадійливою тенденцією. Так, у трьох конференціях з питань комп'ютерної злочинності у Вюрцбурзі в жовтні 1992 р. взяли участь делегати з Африки, Азії, Східної та Західної Європи, Латинської Америки, Близького Сходу та Північної Америки.

Восьмий конгрес ООН з питань запобігання злочинності та поводження з правопорушниками.

За результатами Сьомого конгресу ООН з питань запобігання злочинності та поводження з правопорушниками (1985), Генеральний секретар підготував доповідь «Пропозиції щодо узгоджених міжнародних дій проти форм злочинності, визначених у Міланському плані дій» (E/AC.57/1988/16). Комп’ютерна злочинність обговорювалась у пунктах 42-44 цього звіту.

На своєму 13-му пленарному засіданні Конгрес прийняв резолюцію, в якій, серед іншого, закликав держави-члени активізувати свої зусилля по боротьбі з комп'ютерною злочинністю, розглядаючи, за необхідності, такі заходи:

Модернізація національного кримінального законодавства та процедур, включаючи заходи щодо:

* забезпечення належного застосування існуючих правопорушень та законів, що стосуються повноважень слідства та допустимості доказів у судовому провадженні, та, за необхідності, внести відповідні зміни;
* за відсутності законів, які адекватно застосовуються, слід законодавчо закріпити склади правопорушень, слідчі та доказові процедури.

В 1989 р., розширюючи роботу, яку проводила ОЕСР, Європейський комітет з проблем злочинності Ради Європи підготував набір керівних принципів для національних законодавців, які містили перелік дій в комп’ютерному середовищі, які повинні бути криміналізованими.

Водночас, був розроблений важливий принцип: визначення критеріїв, які б розмежовували «кримінальне діяння» та «зловживання правом» чи «настирливою поведінкою», які не містять елементів складу злочину, в т.ч. «випадкове зловживання комп'ютерною системою», «необережне використання комп'ютерної системи» від «передбачуваного», несанкціонований доступ до комп'ютерної системи цілеспрямований чи випадковий.

Настирливу та необережну чи невмілу поведінку слід чітко відрізняти від злочинної поведінки в законі.

Комітетом ООН з запобігання кіберзлочинам було розроблено «Посібник Організації Об’єднаних Націй з питань запобігання та контролю за комп’ютерною злочинністю», який наразі є міжнародним стандартом запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Посібник містить розділи, які є змістовними, процедурними та організаційними міжнародними стандартами та містять рекомендації для різних країн.

Серед них:

1. Вступ, в якому вирішуються питання та визначаються: а) міжнародна проблема кіберзлочинності; б) регіональні дії в напрямку запобігання кіберзлочинам; в) обгрунтування необхідності глобальних дій.
2. Феномен компютерної злочинності: а) визначення комп’ютерної злочинності; б) масштаби злочинності та втрати; в) винуватці комп'ютерних злочинів (злочинці та правопорушники); г) вразливість комп'ютерних систем до злочинів; д) поширені види комп’ютерних злочинів.
3. Матеріальний кримінальний закон про захист даних власників та інформації: а) передумови порушень; б) розвиток національного права; в) питання міжнародної гармонізації кримінального права.
4. Матеріальне кримінальне законодавство про захист конфіденційності: а) розвиток національного законодавства щодо захисту персональних даних та конфіденційної інформації; б) питання міжнародної гармонізації з питань захисту конфіденційності та персональних даних.
5. Процесуальне (процедурне) законодавство: а) примусові повноваження органів прокуратури; б) конкретні проблеми з персональними даними, їх захистом, порушенням прав на них та запобігання та боротьба з діянняи, якими порушуються права їх валсників в кіберпросторі; в) допустимість комп’ютерних доказів (глобальне вирішення питань електронних доказів: їх виявлення, вилучення, огляд, оцінка та зберігання); допустимість та належність електронних доказів; г) міжнародна гармонізація процесуальних норм щодо застосування єдиних підходів до вирішення процедурних питань поводження з електронними доказами.
6. Профілактика (запобігання) злочинів в компютерному середовищі: а) кібербезпека (безпека в середовищі електронної обробки даних); б) активи та діяльнсть з запобігання компютерним злочинам; в) застосування заходів безпеки; г) правоохоронна та юридична підготовка (підготовка професійна (програмування) та юридична, спеціальна правоохоронна); д) співпраця жертв у повідомленні про комп’ютерні злочини; е) формування та розвиток комп’ютерної етики; є) міжнародна безпека інформаційних систем.
7. Міжнародне співробітництво: а) загальні аспекти; б) питання про юрисдикцію; в) транскордонний пошук комп’ютерних банків даних; г) взаємодопомога в запобіганні, протидії, боротьбі та розслідуванні транскордонних комп’ютерних злочинів; д) екстрадиція; е) передача провадження у кримінальних справах; є) підсумкові зауваження та пропозиції.
8. Висновки.

Висновок однозначний, - є потреба в спільних діях різних держав, міжнародному співробітництві в сфері запобігання компютерним злочинам, та, зокрема, у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку: 1) визначення кіберзлочину та його видів; 2) формування єдиних підходів матеріального кримінального законодавства в країнах; 3) визначення єдиних підходів кримінального процесуального законодавства з питань правового режиму електронних доказів (виявлення, збирання, оцінки, допустимості та належності доказів); виявлення та розслідування кіберзлочинів; застосування запобіжних заходів для збереження матеріальних активів, грошових коштів та інших ресурсів, інформації, інформаційних систем, баз даних та ін.; 4) узгодження юрисдикційних питань та екстардиції; 5) взаємна допомога та спільне проведення слідчих та запобіжних правоохоронних заходів, спрямованих на попередження та розкриття злочинів, виявлення винних осіб та притягнення їх до кримінальної відповідальності; 6) проведення спільних заходів з підготовки фахівців, обміну інформацією та їх взаємодії.

Як вже зазначалося, Україна зробила важливий крок, прийнявши Закон України «Про основні засади забезпечення кібербезпеки України», та визначивши в ньому пріоритетність питань: а) кібербезпеки, - як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі; б) кіберзагроз, - як наявних та потенційно можливих явищ і чинників, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів; в) кіберзахисту, - як сукупності організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Міжнародною спільнотою вироблено стандарти протидії (запобігання) кіберзагрозам (відповідно і кіберзлочинам). Такими є: Міжнародний стандарт управління інформаційною безпекою серії ISO/IEC 27001 «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційної безпеки - Вимоги», призначений для захисту даних від кіберзлочинності, керування інформаційною безпекою та притягнення злочинців до відповідальності; міжнародний стандарт для управління інформаційної безпеки: ISO/IEC 17799: 2005 - «Інформаційні технології - Технології безпеки - Практичні правила управління інформаційної безпеки», а зараз, - ISO/IEC 17799: 2005. «Інформаційні технології - Технології безпеки - Практичні правила управління інформаційної безпеки»; ISO 13335 Міжнародні стандарти безпеки інформаційних технологій, які містять чотири стандарти; ISO / IEC 15408-1: 2009 Інформаційні технології. Методи забезпечення безпеки. Критерії оцінки безпеки ІТ; CRAMM Version 5.0 (метод аналізу та управління ризиками CCTA) – методологія управління ризиками.

Зараз триває розробка нового стандарту у сфері інформаційної безпеки - ISO/IEC 27552 «Методи захисту. Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління інформацією про конфіденційність. Вимоги та керівні вказівки», який додатково розширює ISO/IEC 27001 для вирішення конкретних потреб у сфері конфіденційності.

Загалом же, забезпечення інформаційної безпеки відбувається за трьома напрямками: технічному, адміністративному та організаційному.

На сьогодні в ЄС особливу роль в вирішенні питань протидії протиправним посяганням на доступ до електронних сервісів інформаційних систем (ДЕІР) та інші ресурси, відіграють: а) Директива ЄС щодо протидії кібератакам на інформаційні системи (2013 р.); б) Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет, (2017 р.); в) Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації» (Network and Information Security), що набрав чинності 09.05.2018 р., який встановлює правила роботи з персональними даними (GDPR) і ставить досить жорсткі вимоги до технічної складової захисту персональних даних.

В Україні правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Указ Президента України № 92/2016 «Про рішення Ради національної безпеки і оборони України від 04.03.2016 року «Про Концепцію розвитку сектору безпеки і оборони України»» та ін.

Основна увага в ЄС та країнах ЄС приділяється питанням раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти ДЕІР. Тому до Стратегії кібербезпеки Європейського Союзу у поняття «кіберзахист» додано виявлення і блокування кібератак, локалізацію їх наслідків незалежно від походження стосовно цивільних об’єктів усіх форм власності, а також встановлення і розслідування кіберзлочинів.

Виконання цієї функції в ЄС покладено на Європейську агенцію мережевої та інформаційної безпеки (European Net­work and Information Security Agency, ENISA).

Безпосереднє виявлення кібератаки за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів забезпечується структурою СERT-EU (Computer Emergency Response Team). У випадку кібератаки датчики (система та комп’ютерна програма, що містить фільтри) сповіщають СERT-EU про ймовірну загрозу та ризики. CERT-EU. Аналізуючи дані, у випадку виявлення кібератаки з ознаками злочинних дій, передає інформацію до Європейського центру з розслідуван­ня кіберзлочинів (European Cybercri­me Centre, ECС), який у надзвичайних випадках при ймовірності істотної загрози інформує про неї Європейську агенцію оборони (European Defence Agency) для організації кібер­операцій та Європейську службу зовнішніх справ (European External Action Service).

США має трошки іншу структуру: з 2007 р. запроваджену систему (програму) Довірчих ін­тернет-з’єднань (TIC, Trusted Internet Connections), яка забезпечує безпеку близько 5.000 компютерних мереж та інформаційних систем органів федеральної влади США.

Головною структурою з забезпечення кіберзахисту в США є Національний центр кібербезпеки та інтеграції зв’язку (NCCIC, National Cy­bersecurity and Communication Integ­ration Center), до складу якого входять: 1) група екстреного реагування на комп’­ютерні події в США (US-CERT, U.S. Computer Emergency Response Team); 2) група екстреного реагування на надзвичайні події у системах управління промисловістю (ICS-CERT, Industrial Control Systems Cyber Emergency Res­ponse Team); 3) Національний координаційний центр зв’язку (NCC, National Coordinating Center for Communica­tions).

US-CERT виявляє кібератаки на об’єктах федеральних органів влади США і попереджає про них адміністраторів безпеки інформаційних систем, координує їх діяльність з протидії загрозам та відновлення федеральних інформаційних систем після кібератак або кіберінцидентів.

ICS-CERT попереджає і виявляє кібератаки на інформаційні системи об’єктів критичної інфраструктури в промисловості США.

В листопаді 2018 року Указом Президента США Національний центр кібербезпеки та інтеграції зв’язку (NCCIC) було передано у підпорядкування нового агентства з кібербезпеки та безпеки інфраструктури міністерства внутрішньої безпеки США.

В Україні з урахуванням досвіду ЄС і США розбудовуєть­ся мережа ситуаційних центрів кіберзахисту на об’єктах критичної інформаційної інфраструктури та система ситуаційних центрів кібербезпеки в основних суб’єктах системи забезпечення кібербезпеки (СБУ, Національної поліції України, Міністерстві оборони України, СЗР, Головного управління розвідки МОУ).

Фахівці визначають, що захист та протидія протиправним посяганням на ДЕІР має проблеми, які потребують нормативного та організаційного вирішення. Основною проблемою є те, що Україна, намагаючись співпрацювати з іноземними державами та міжурядовими організаціями, не імплементуючи повноцінно положення Конвенції про кібер­злочинність через недолугість кримінального процесуального законодавства України, позбавлена можливості ефективно забезпечувати кібербезпеку та реакцію на кіберзагрози.

Головною проблемою наразі є невідповідність системи збирання електронних доказів, та й, взагалі відсутність категорії «електронний доказ» в КПК України. Законодавство більшості країн-учасниць зазначеної Конвенції містить положення про особливий порядок перехоплення і розкриття інформації про рух даних у комп’ютерних системах задля розслідування кіберзлочинів та з метою оперативного припинення кіберзлочину та ліквідації його наслідків.

Згідно ж чинного Кримінального процесуального кодек­су України для отримання інформації від операторів і провайдерів, необхідної для припинення злочину або встановлення винних у його вчиненні, ліквідації негативних наслідків від кримінального правопорушення, та, більш того, блокування (обмеження) ресур­су з протиправним контентом, правоохоронні органи витрачають цінний час для одержання відповідного рішення суду в межах кримінального провадження.

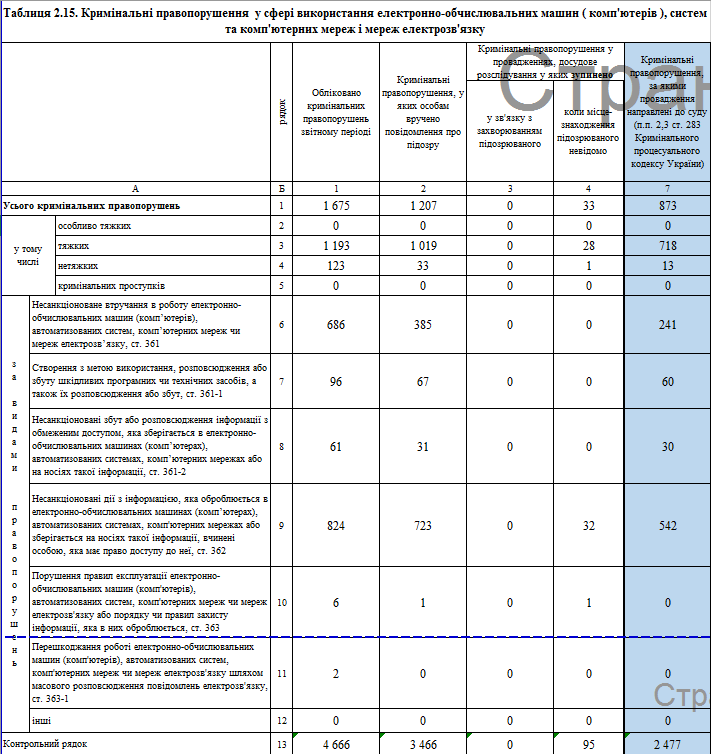
Ця проблема може бути вирішена виключно шляхом законодавчого закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку і арешту електронних доказів, та, в першу чергу, закріплення процесуальної можливості та порядку копіювання, зберігання, поводження та використання інформації.

*Апробація результатів дослідження.* Результати кваліфікаційної роботи були обговорені на засіданнях кафедри конституційного та трудового права Запорізького національного університету. Положення даної магістерської роботи були враховані автором в ході підготовки наукових статей для опублікування в українській наукові періодиці, під час участі у роботі наукових конференцій: VІІІ Міжнародній заочній науково-практичній конференції «Формування ефективних механізмів державного управління та менеджменту в умовах сучасної економіки: теорія і практика» (27.11.2020 р., м. Запоріжжя), Міжнародній науково-практичній конференції «Правові системи суспільства: сучасні проблеми та перспективи розвитку» (м. Львів, 20–21 листопада 2020 р.).

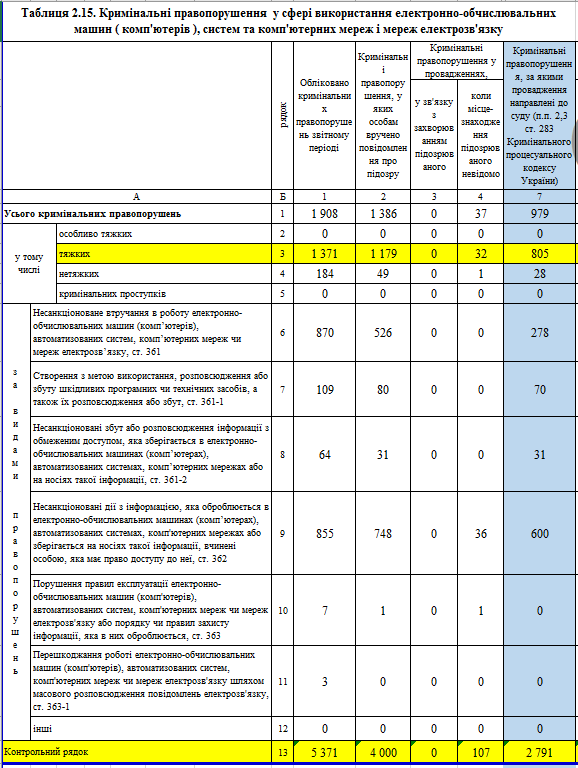
РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА

2.1 Стан злочинності у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

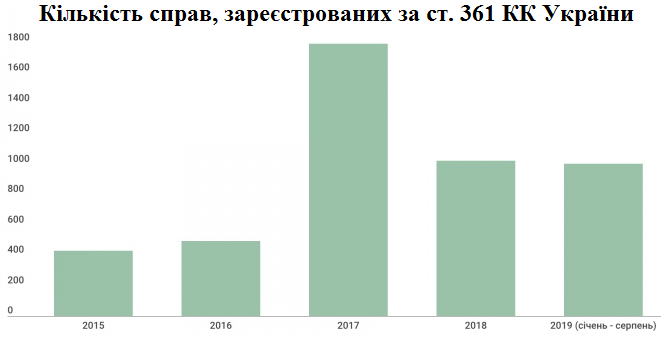
Стан виявлення та розкриття кіберзлочинів за даними Генеральної прокуратури України (серпень 2020 р.)



Стан виявлення та розкриття кіберзлочинів за даними Генеральної прокуратури України (вересень 2020 р.)



Показники зростання кіберзлочинності



2.2 Види злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

Кіберзлочини, закріплені в Кримінальному Кодексі України

несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку(ст. 361 КК України)

створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 3611 КК України)

несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України)

несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України)

порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України)

перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України)

Класифікація кіберзлочинів

згідно з Конвенцією Ради Європи по боротьбі з кіберзлочинністю

1. Злочини проти конфіденційності, цілісності та до­ступності комп’ютерних даних і систем

* несанкціонований доступ до інформаційного середо­вища, здійснений шляхом протиправного навмисного доступу до комп’ютерної системи або її частини, вченений в обхід систем безпеки;
* незаконне перехоплення – протиправне нав­мисне перехоплення не призначених для загального досту­пу комп’ютерних даних, які передаються комп’ютерними системами, яке здійснюється шляхом використання технічних засобів в обхід заходів безпеки;
* втручання в дані - протиправна зміна, пошкодження, ви­далення, спотворення або блокування комп’ютерних даних;
* втручання в роботу системи - протиправне порушен­ня або створення перешкод функціонуванню комп’ютерної системи;
* незаконне використання комп’ютерного і телекому­нікаційного устаткування - виготовлення, придбання для використання, поширення або надання доступу:

а) пристроїв та комп’ютерних програм, розроблених або пристосованих для здійснення зло­чинів;

Класифікація кіберзлочинів

згідно з Конвенцією Ради Європи по боротьбі з кіберзлочинністю

1. Шахрайство та підробка, що пов’язані з використан­ням комп’ютерів:

* підробка документів із застосуванням комп’ютерних засобів - протиправне умисне внесення, зміна, видалення або блокування комп’ютерних даних, що призводить до зниження їхньої достовірності, припускає, що згодом вони розглядатимуться як достовірні;
* шахрайство із застосуванням комп’ютерних засобів - втручання у функціонування комп’ютерної системи з об­манним або нечесним наміром умисного протиправного отримання економічної вигоди для себе або для інших осіб.

б) комп’ютерних паролів, кодів доступу, інших даних, які забезпечують доступ до комп’ютерної систе­ми або її частини за наявності наміру використання їх з метою здійснення будь-якого із зазначених вище злочинів; володіння одним із перелічених предметів із наміром використати його для здійснення будь-якого зі злочинів.

Класифікація кіберзлочинів

згідно з Конвенцією Ради Європи по боротьбі з кіберзлочинністю

3. Злочини, пов’язані з розміщенням у мережах проти­правної інформації:

4. Злочини проти авторських і суміжних прав

Злочини щодо авторських і суміжних прав, які здійснюються шляхом викорис­танням комп’ютерної системи злочини щодо прав, передбачених низкою відповідних міжнародних актів щодо захисту авторських та суміжних прав та інших об’єктів права інтелектуальної власності.

злочини, пов’язані з дитячою порнографією, - по­ширення дитячої порнографії за допомогою глобальних мереж, пропозиція або надання доступу до неї, отримання для себе або інших осіб за допомогою комп’ютерної сис­теми, зберігання дитячої порнографії в комп’ютерній сис­темі

Класифікація «цифрових злочинів» («digital crime») згідно інструктивних матеріалах Інтерполу

1) комп’ютерні злочини (порушення авторських прав на програмне забезпечення, розкрадання даних, пору­шення роботи обчислювальних та інформаційних комп’ютерних систем, розкрадання комп’ю­терного часу та ін.)

3) мережева злочинність (використання мереж для здійснення незаконних угод, в т.ч. поши­рення порнографії, торгівлі наркотиками, ухилення від митних зборів, відмивання грошей та ін.).

2) злочини, «пов’язані з комп’ютерами» (фінансове шахрайство)

Класифікація «цифрових злочинів» («digital crime») згідно інструктивних матеріалах Інтерполу

QA- несанкціонований доступ і перехоплення;

QAH - комп’ютерний абордаж (несанкціонований до­ступ);

QAI - перехоплення за допомогою спеціальних техніч­них засобів;

QAT - крадіжка часу (ухилення від плати за користу­вання);

QAZ - інші види несанкціонованого доступу та пере­хоплення;

QD - зміна комп’ютерних даних;

QDL - логічна бомба;

QDT - троянський кінь;

QDV - комп’ютерний вірус;

QDW - комп’ютерний черв’як;

QDZ - інші види зміни даних;

QF - комп’ютерне шахрайство;

QFC - шахрайство з банкоматами;

QFF - комп’ютерна підробка;

QFG - шахрайство з ігровими автоматами;

QFM - маніпуляції з програмами введення-виведення;

QFP - шахрайства з платіжними засобами;

QFT - телефонне шахрайство;

QFZ - інші комп’ютерні шахрайства;

QR - незаконне копіювання;

QRG - комп’ютерні ігри;

QRS - інше програмне забезпечення;

QRT - топологія напівпровідникових пристроїв;

QRZ - інше незаконне копіювання;

QS - комп’ютерний саботаж;

QSH - з апаратним забезпеченням (порушення роботи ЕОМ);

QSS - із програмним забезпеченням (знищення, блоку­вання інформації);

QSZ - інші види саботажу;

QZ - інші комп’ютерні злочини;

QZB - із використанням комп’ютерних дошок оголо­шень;

QZE - розкрадання інформації, що становить комерцій­ну таємницю;

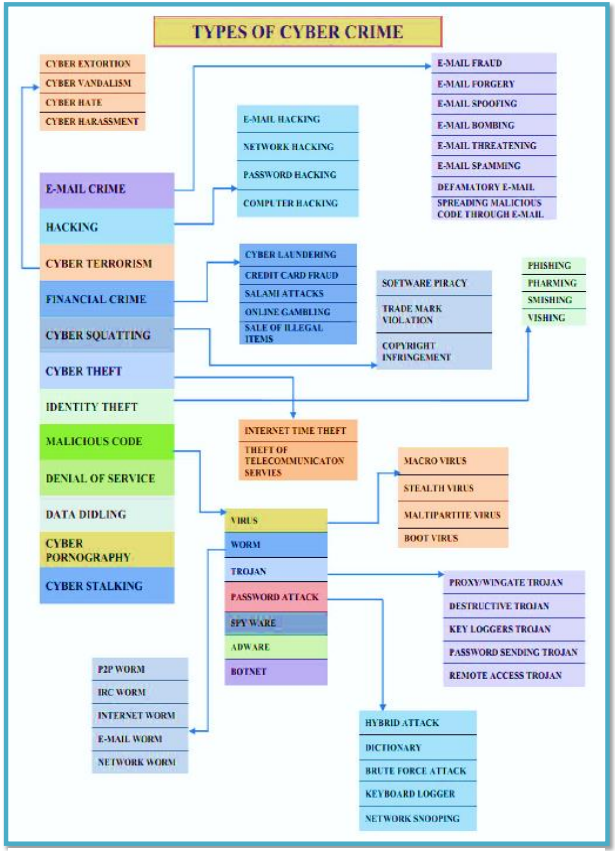
QZS - передача інформації, що підлягає судовому роз­гляду;

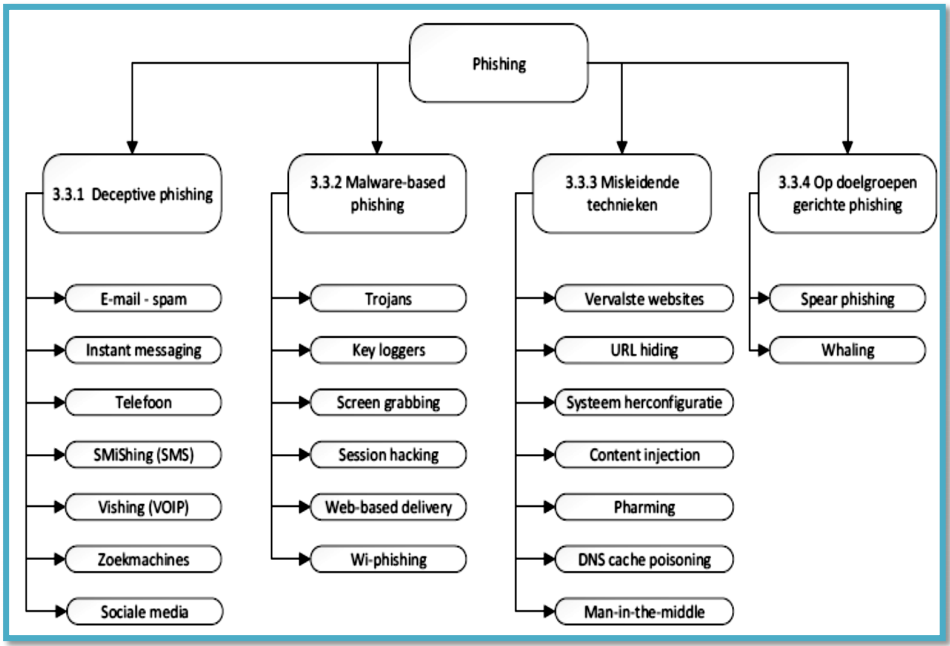
QZZ - інші комп’ютерні злочини.

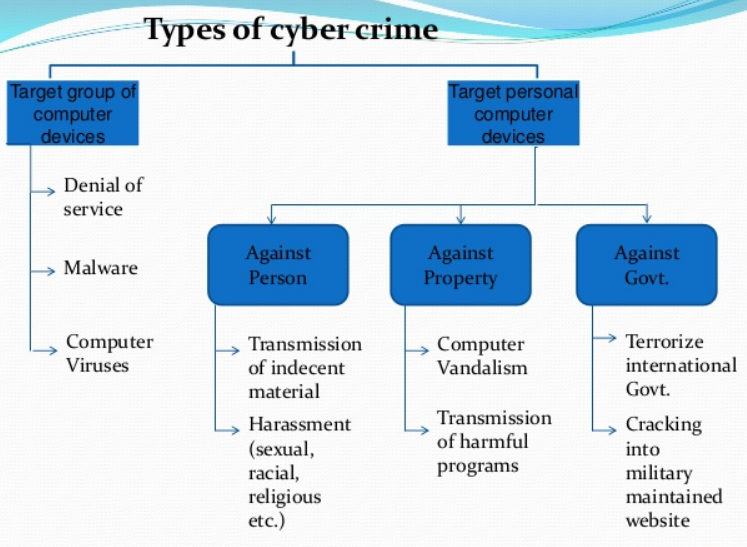
Класифікації «цифрових злочинів» («digital crime»), комп’ютерних злочинів чи кіберзлочинів

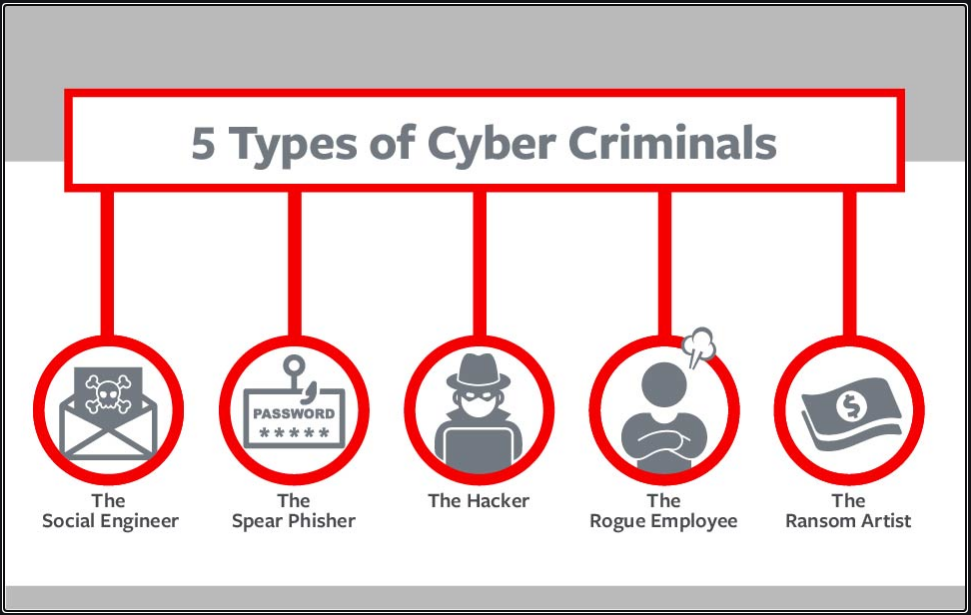
* насильницькі або інші потенційно небезпечні дії, що посягають на фізичну безпеку, життя та здоров’я людини;
* дії, що порушують конфіденційність даних, які містяться чи передаються в інформаційних і телекомунікаційних системах (ці злочини спрямовані на розкриття інформації без зміни її змісту);
* дії, що порушують цілісність даних, їхню доступ­ність для адміністраторів і легальних користувачів (відмо­ва в обслуговуванні), що здатне порушити штатні режими функціонування інформаційних і телекомунікаційних сис­тем різного призначення (злочини, що заподіюють майнові збитки через збій чи зупинку функціонування комп’ютерних систем чи комп’ютерних мереж. Не пов’язані з розкраданням інформації чи грошових коштів);
* дії, що посягають на майно, майнові права, а також на право власності, прав на інформацію чи авторські права;
* дії, що посягають на громадську моральність;
* дії, що посягають на громадську безпеку;
* інші.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Види кіберзлочинів | | | | | |
| Кардинг | шахрайські операції з кредитними картками, не погоджені власником картки (несанкціоновано, без повноважень): крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки | | | | Мета: отримання доступу до чужих грошових коштів |
| Основний спосіб: фішинг, - використання необізнаності, довірливості та неуважності власника картки |
| Фішинг | шахрайські дії, спрямовані на виманювання реквізитів картки чи /та її рахунку і інформації доступу до нього (логін/пароль) у її власника. Як правило, власник кредитної чи дебетової картки добровільно повідомляє шахраям таку інформацію | | | | |
|  | СМС-фішинг | | потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку | | |
|  | Інтернет-фішинг | | шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів і т.п. Основна причина стати жертвою – легковірність та неуважність | | |
|  | Фішинг на основі зловмисного програмного забезпечення | | використання шкідливого програмного забезпечення для прив’язки до комп’ютера жертви з метою надсилання хакеру конфіденційних даних жертви | | |
|  | Trojans (троянські програми) | | шкідлива комп’ютерна програма, яка видає себе корисною, рутинною або цікавою для того, щоб переконати жертву встановити її. Якщо його встановити або запустити з підвищеними привілеями, троянець, як правило, матиме необмежений доступ. Що він робить з цією владою, залежить від мотивів нападника | | |
|  | Key loggers (Реєстратори клавіш) | | форма шкідливого програмного забезпечення, яка фіксує та ідентифікує кожне натискання клавіші, набране на певній клавіатурі. Всю набрану інформацію може отримати інша особа, навіть якщо автор змінює або видаляє те, що було написано, або якщо символ не з’являється на моніторі, наприклад, при введенні пароля. Вхідні дані надсилаються хакерам, які намагаються розшифрувати всілякі паролі та інші типи інформації з усіх вхідних даних, які вони отримують | | |
|  | Screen Grabbing (Захоплення екрану) | | деякі розширені фішинг-атаки роблять скріншоти даних, які вводяться, наприклад, у веб-програму. Цей тип шкідливого програмного забезпечення використовується, щоб обійти безпеку програм, що забезпечуються анти-клавішними реєстраторами | | |
|  | Web-Based Delivery (Доставка через Інтернет) | | ця форма фішингу на основі шкідливого програмного забезпечення трапляється, коли жертва натискає посилання у фішинг-повідомленні та переходить на веб-сайт. Цей веб-сайт при відкритті встановить шкідливе програмне забезпечення на комп’ютер жертви. Як тільки жертва використовує комп’ютер для виконання деяких транзакцій, шкідливе програмне забезпечення перенаправить дані на фішер | | |
|  | Session hacking (Злом сеансу) | | фішер використовує переваги керованості веб-сеансів. Простий «сеансовий злом» дозволяє фішеру скористатися засобом пошуку для перехоплення відповідної інформації, щоб порушник міг надати нелегальний доступ до самого веб-сервера | | |
|  | Wi-phishing | | встановлення точки доступу Wi-Fi для того, щоб користувачі мобільних пристроїв могли автоматично підключатись до своїх точок вимірювання до цієї точки доступу. Тим часом на приладі буде встановлено шкідливе програмне забезпечення або викрадено дані з мобільних пристроїв. Оскільки в громадських місцях встановлюється все більше і більше безкоштовних точок доступу Wi-Fi, фішер легко використовувати іншу назву мережі Wi-Fi (SSID), щоб заманити користувача до точки доступу до Wi-Fi | | |
|  | On target-specific phishing (фішинг, що має конкретну мету) | | Spear-phishing (спір-фішинг) | ретельно вибирається не засіб, а жертва. Зловмисник намагається зібрати якомога більше інформації про ціль, і оманливий характер повідомлення про фішинг посилиться та збільшить рівень успіху атаки. Збір інформації використовується для пошуку вразливостей (наприклад, особистої інформації в соціальних мережах), злому файлу або веб-сайту клієнта, щоб обдурити жертву | |
|  | Whaling (китобійний промисел) | є особливою формою «підводного» фішингу, коли злочинець вибирає цілями компанії, уряди або групи керівників високого рівня. Фішер намагається напасти на невелику групу вищих посадових осіб, щоб зірвати його, щоб він міг витратити більше часу на атаку та вдосконалити своє повідомлення до найвищого рівня успіху, щоб досягти успіху | |
| Вішинг | Схема, наближена до фішингу, яка полягає в виманюванні реквізитів картки злочинці здійснюють за допомогою телефонних дзвінків (шахраї представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити певні дії за власним рахунком) | | | | |
| Скімінг | Схема: копіювання даних платіжної картки за допомогою скімера (спеціального пристрою). Для отримання даних злочинці використовують міні-камери або змінні клавіатури, які навісно встановлюються злочинцями на банкомат | | | | |
| Шимінг | модернізований різновид скімінгу | | Схема: злочинці використовують майже непомітний прилад, який розміщують всередині картридера, що дозволяє копіювати дані платіжної картки копіювати непомітно | | |
| Онлайн-шахрайство | фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв'язку | | | | |
| Піратство | Схема: протиправне розповсюдження об'єктів права інтелектуальної власності в Інтернеті | | | | |
| Мальваре | створення та поширення вірусів та іншого шкідливого програмного забезпечення | | | | |
| Рефайлінг | незаконна підміна телефонного трафіку | | | | |
| Розповсюдження протиправного контенту | Розповсюдження протиправного контенту, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства | | | | |
| Нові види кіберзлочинів, визначені Інтерполом | | | | | |
| Cyber Terrorism (кібертероризм) | Дія: вторгнення в роботу комп’ютерних мереж чи мереж електрозв’язку, що здійснюється переважно організованими діями кібертерористів, іноземних спецслужб або інших груп.  Мета: 1 – виявлення потенційних прогалин в безпеці в критичних системах.  Мета: 2 – залякування чи примушування уряду чи організації досягати своїх політичних чи соціальних цілей, здійснюючи комп'ютерну атаку на комп'ютери, мережі чи інформацію, що зберігається на них. | | | | |
| «Сyberhate» (кіберхайту) | Пропаганда расизму та Голокосту, виправдання або схвалення геноциду, скоєного під час Другої світової війни, розв’язування міжнаціональної чи релігійної ворожнечі  Може поєднуватися з залякуванням в Інтернеті, образами або насильством на основі будь якої дискримінаційної ознаки.  Дискримінація за будь-якою ознакою: ознакою статі, сексуальної орієнтації, релігії чи життєвої філософії. | | | | |
| Cyberextortion - Кіберекстрація | злочин, пов’язаний з нападом або загрозою нападу у поєднанні з попитом. В Інтернет-сленгу «троль» - це людина, яка сіє розбрат в Інтернеті, висловлюючи суперечки або засмучуючи людей, публікуючи запальні, сторонні повідомлення або повідомлення, що не стосуються теми.  Як правило, здійснюється Інтернет-спільнотою на блоках новин, форумах, в чатах або в блогах з навмисним наміром викликати читачів на емоційний відгук, негативне ставлення до інформації, подій, дій державних органів, політиків; роботи, товарів чи послуг певних організацій або іншим чином порушити нормальну дискусію на тему, часто для власної розваги. | | | | |
| Може здійснюватися з метою вимоги грошей за припинення тролінгу | Способи:   1. напади на корпоративні веб-сайти для відмови в обслуговуванні (DoS) (пінг-шторм) з наступною вимогою внести гроші на банківський рахунок в іноземній країні в обмін на припинення нападу 2. Змінено на програми-вимагачі, які шифрують дані жертви. Жертва отримує електронне повідомлення, яке пропонує приватний ключ розшифровки в обмін на грошовий платіж у біткойнах. Оплата не гарантує дешифрування та припинення атак. Ініціюється через зловмисне програмне забезпечення у вкладеннях електронної пошти або на скомпрометованих веб-сайтах | | | |
| Cyberbullying - Кібер-знущання | дії, що використовують інформаційно-комунікаційні технології для підтримки навмисної, повторюваної та ворожої поведінки окремої особи чи групи, яка має на меті завдати шкоди іншій особі чи іншим особам | | | | |
| використання комунікаційних технологій з метою заподіяння шкоди іншій особі чи іншим особам | | | | |
| використання Інтернет-послуг та мобільних технологій, таких як веб-сторінки та дискусійні групи, а також обмін миттєвими повідомленнями або SMS-повідомленнями з метою заподіяння шкоди іншій особі чи іншим особам | | | | |

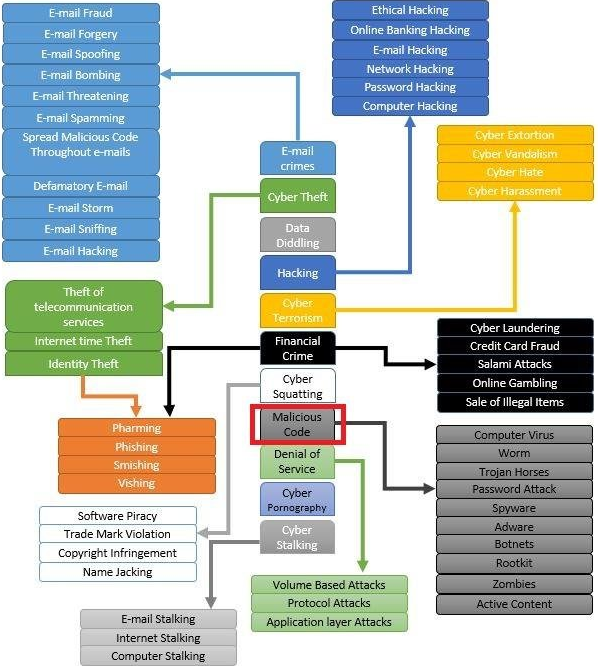


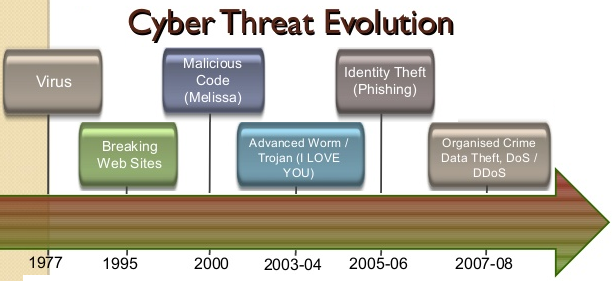












2.3 Нормативне регулювання запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

Нормативні акти з протидії злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

Міжнародні

Національні

Конвенція Ради Європи про кіберзлочинність

23.11.2001 р.

Конституція України 1996 р.

Директива ЄС щодо протидії кібератакам на інформаційні системи (2013 р.);

Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет, (2017 р.)

Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації» (Network and Information Security), 09.05.2018 р.

Укази Президента

Кримінальний процесуальний кодекс України 18.04.2010 р.

Закон України «Про основні засади забезпечення кібербезпеки України» 05.10.2017 р.

Закон України «Про національну поліцію» 02.07.2015 р.

Кримінальний кодекс України 05.04.2001 р.

**Стандарти інформаційної безпеки**

**ISO/IEC 27001 «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційної безпеки - Вимоги»**

призначений для захисту даних від кіберзлочинності, керування інформаційною безпекою та притягнення злочинців до відповідальності

**ISO/IEC 17799: 2005 - «Інформаційні технології - Технології безпеки - Практичні правила управління інформаційної безпеки»**

міжнародний стандарт для управління інформаційної безпеки

**CRAMM Version 5.0** (метод аналізу та управління ризиками CCTA) методологія управління ризиками

**ISO 13335 Міжнародні стандарти безпеки інформаційних технологій** (чотири стандарти)

**ISO / IEC 15408-1: 2009 Інформаційні технології. Методи забезпечення безпеки. Критерії оцінки безпеки ІТ**

**ISO/IEC 27552 «Методи захисту. Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління інформацією про конфіденційність. Вимоги та керівні вказівки»**

|  |  |
| --- | --- |
| **ISO / IEC 27000, Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою - Огляд та словниковий запас** | |
| ISO / IEC 27001: 2013 | *Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою - Вимоги* |
| ISO / IEC 27002: 2013 | *Інформаційні технології - Методи безпеки - Кодекс практики управління інформаційною безпекою* |
| ISO / IEC 29100 | *Інформаційні технології - Методи безпеки - Основи конфіденційності* |
| **Система управління інформацією про конфіденційність**  **PIMS** | |
| ISO / IEC 19944 | *Інформаційні технології - Хмарні обчислення - Хмарні послуги та пристрої: Потік даних, категорії даних та використання даних* |
| ISO / IEC 20889 | *Термінологія*деідентифікації даних , що *покращує конфіденційність, та класифікація методів* |
| ISO / IEC 27005 | *Інформаційні технології - Методи безпеки - Управління ризиками інформаційної безпеки* |
| ISO / IEC 27018 | *Інформаційні технології - Методи безпеки - Кодекс практики захисту інформації, що ідентифікує особу (PII), у публічних хмарах, що виконують роль процесорів PII* |
| ISO / IEC 27035-1 | *Інформаційні технології - Методи безпеки - Управління інцидентами інформаційної безпеки - Частина 1: Принципи управління інцидентами* |
| ISO / IEC 29101 | *Інформаційні технології - Методи безпеки - Структура архітектури конфіденційності* |
| ISO / IEC 29134 | *Інформаційні технології - Методи безпеки - Керівництво з оцінки впливу на конфіденційність* |
| ISO / IEC 29151 | *Інформаційні технології - Методи безпеки - Кодекс практики захисту інформації, що ідентифікує особу* |
| ISO / IEC / DIS 29184 | *Інформаційні технології - Методи безпеки - Вказівки щодо повідомлень про конфіденційність та згоди в Інтернеті* |

|  |
| --- |
| **ISO/IEC 27001:2013(en)** Information technology - Security techniques - Information security management systems - Requirements |
| **ISO/IEC 27001:2013**(en) Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою - Вимоги |
| ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) |
| ISO (Міжнародна організація зі стандартизації) та IEC (Міжнародна електротехнічна комісія) утворюють спеціалізовану систему світової стандартизації. Національні органи, які є членами ISO або IEC, беруть участь у розробці міжнародних стандартів через технічні комітети, створені відповідною організацією для розгляду конкретних галузей технічної діяльності. Технічні комітети ISO та IEC співпрацюють у сферах, що становлять взаємний інтерес. Інші міжнародні організації, урядові та неурядові, у взаємодії з ISO та IEC, також беруть участь у роботі. У галузі інформаційних технологій ISO та IEC створили спільний технічний комітет ISO / IEC JTC 1.  Міжнародні стандарти розробляються відповідно до правил, наведених у Директиві ISO / IEC, частина 2.  Основним завданням спільного технічного комітету є підготовка міжнародних стандартів. Проекти міжнародних стандартів, прийняті спільним технічним комітетом, розсилаються національним органам для голосування. Публікація як міжнародний стандарт вимагає схвалення принаймні 75% національних органів, які проголосували.  Звертається увага на можливість того, що деякі елементи цього документа можуть бути предметом патентних прав. ISO та IEC не несуть відповідальності за ідентифікацію будь-яких або всіх таких патентних прав.  ISO / IEC 27001 був підготовлений Спільним технічним комітетом ISO / IEC JTC 1, Інформаційні технології , Підкомітет SC 27, Методи ІТ-безпеки .  Це друге видання скасовує та замінює перше видання ( ISO / IEC 27001: 2005 ), яке було технічно переглянуто. |

|  |
| --- |
| **ISO/IEC 27002:2013(en)**  Information technology — Security techniques — Code of practice for information security controls |
| **ISO/IEC 27002:2013(en)**  Інформаційні технології - Методи безпеки - Звід практики управління інформаційною безпекою |
| Передмова |
| 0 Вступ |
| 1 Сфера застосування |
| 2 Нормативні посилання |
| 3 Терміни та визначення |
| 4 Структура цього стандарту |
| 4.1 Статті |
| 4.2 Контрольні категорії |
| 5 Політика інформаційної безпеки |
| 5.1 Напрямок управління інформаційною безпекою |
| 6 Організація інформаційної безпеки |
| 6.1 Внутрішня організація |
| 6.2 Мобільні пристрої та робота на дистанції |
| 7 Безпека людських ресурсів |
| 7.1 До працевлаштування |
| 7.2 Під час працевлаштування |
| 7.3 Припинення та зміна роботи |
| 8 Управління активами |
| 8.1 Відповідальність за активи |
| 8.2 Класифікація інформації |
| 8.3 Обробка носіїв |
| 9 Контроль доступу |
| 9.1 Бізнес-вимоги контролю доступу |
| 9.2 Управління доступом користувачів |
| 9.3 Обов'язки користувача |
| 9.4 Контроль доступу до системи та додатків |
| 10 Криптографія |
| 10.1 Криптографічний контроль |
| 11 Фізична та екологічна безпека |
| 11.1 Захищені зони |
| 11.2 Обладнання |
| 12 Операційна безпека |
| 12.1 Оперативні процедури та обов'язки |
| 12.2 Захист від шкідливих програм |
| 12.3 Резервне копіювання |
| 12.4 Протоколювання та моніторинг |
| 12.5 Контроль операційного програмного забезпечення |
| 12.6 Управління технічною вразливістю |
| 12.7 Міркування щодо аудиту інформаційних систем |
| 13 Безпека зв'язку |
| 13.1 Управління безпекою мережі |
| 13.2 Передача інформації |
| 14 Придбання, розробка та обслуговування системи |
| 14.1 Вимоги до безпеки інформаційних систем |
| 14.2 Безпека в процесах розробки та підтримки |
| 14.3 Дані тесту |
| 15 Відносини з постачальниками |
| 15.1 Інформаційна безпека у відносинах з постачальниками |
| 15.2 Управління наданням послуг постачальника |
| 16 Управління інцидентами інформаційної безпеки |
| 16.1 Управління інцидентами та вдосконаленнями інформаційної безпеки |
| 17 Аспекти інформаційної безпеки управління безперервністю бізнесу |
| 17.1 Безперервність інформаційної безпеки |
| 17.2 Звільнення |
| 18 Відповідність |
| 18.1 Дотримання законодавчих та договірних вимог |
| 18.2 Огляди інформаційної безпеки |

|  |
| --- |
| **ISO/IEC 27701:2019(en)**  Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines |
| **ISO/IEC 27701:2019(en)**  Методи безпеки - Розширення до ISO / IEC 27001 та ISO / IEC 27002 для управління інформацією про конфіденційність - Вимоги та керівні принципи |

|  |
| --- |
| Передмова |
|  |
| Вступ |
| 1 Сфера застосування |
| 2 Нормативні посилання |
| 3 Терміни, визначення та скорочення |
| 4 Загальне |
| 4.1 Структура цього документа |
| 4.2 Застосування вимог ISO / IEC 27001: 2013 |
| 4.3 Застосування керівних принципів ISO / IEC 27002: 2013 |
| 4.4 Клієнт |
| 5 Вимоги до PIMS, пов'язані з ISO / IEC 27001 |
| 5.1 Загальні положення |
| 5.2 Контекст організації |
| 5.3 Лідерство |
| 5.4 Планування |
| 5.5 Підтримка |
| 5.6 Експлуатація |
| 5.7 Оцінка результативності |
| 5.8 Удосконалення |
| 6 Спеціальні вказівки щодо PIMS, що стосуються ISO / IEC 27002 |
| 6.1 Загальні положення |
| 6.2 Політика інформаційної безпеки |
| 6.3 Організація інформаційної безпеки |
| 6.4 Безпека людських ресурсів |
| 6.5 Управління активами |
| 6.6 Контроль доступу |
| 6.7 Криптографія |
| 6.8 Фізична та екологічна безпека |
| 6.9 Безпека операцій |
| 6.10 Безпека зв'язку |
| 6.11 Придбання, розробка та обслуговування систем |
| 6.12 Взаємовідносини з постачальниками |
| 6.13 Управління інцидентами інформаційної безпеки |
| 6.14 Аспекти інформаційної безпеки управління безперервністю бізнесу |
| 6.15 Відповідність |
| 6.3 Організація інформаційної безпеки |
| 6.4 Безпека людських ресурсів |
| 6.5 Управління активами |
| 6.6 Контроль доступу |
| 6.7 Криптографія |
| 6.8 Фізична та екологічна безпека |
| 6.9 Безпека операцій |
| 6.10 Безпека зв'язку |
| 6.11 Придбання, розробка та обслуговування систем |
| 6.12 Взаємовідносини з постачальниками |
| 6.13 Управління інцидентами інформаційної безпеки |
| 6.14 Аспекти інформаційної безпеки управління безперервністю бізнесу |
| 6.15 Відповідність |
| 7 Додаткові вказівки ISO / IEC 27002 для контролерів ідентифікації персональних даних |
| 7.1 Загальні положення |
| 7.2 Умови збору та переробки |
| 7.3 Зобов'язання перед керівниками ІВС |
| 7.4 Конфіденційність за дизайном та конфіденційність за замовчуванням |
| 7.5 Обмін, передача та розкриття інформації, що охороняє інформацію |
| 8 Додаткові вказівки ISO / IEC 27002 для процесорів PII |
| 8.1 Загальні положення |
| 8.2 Умови збору та переробки |
| 8.3 Зобов'язання перед керівниками ІВС |
| 8.4 Конфіденційність за дизайном та конфіденційність за замовчуванням |
| 8.5 Обмін, передача та розкриття інформації, що охороняє інформацію |
| Додаток A, специфічні для PIMS цілі та засоби контролю (контролери PII) |
| Додаток B Специфічні для PIMS цільові контрольні цілі та засоби управління (PII-процесори) |
| Додаток С Картування до ISO / IEC 29100 |
| Додаток D Картування до Загального регламенту захисту даних |
| Додаток Е Картування до ISO / IEC 27018 та ISO / IEC 29151 |
| Додаток F Як застосовувати ISO / IEC 27701 до ISO / IEC 27001 та ISO / IEC 27002 |
| F.1 Як застосовувати цей документ |
| F.2 Приклад уточнення стандартів безпеки |

**Акти національного законодавства в сфері кібербезпеки**

Конституція України

Кримінальний Кодекс України

Кримінальний процесуальний Кодекс України

Закон України «Про основні засади забезпечення кібербезпеки України» 05.10.2017 р.

Закон України «Про інформацію» 02.10.1992 р.

Закон України «Про телекомунікації» 18.11.2003 р.

Закон України «Про Службу безпеки України» 25.03.1992 р.

Закон України «Про національну поліцію» 02.07.2015 р.

Закон України «Про національну безпеку України» 21.06.2018 р.

Закон України «Про оперативно-розшукову діяльність» 18.02.1992

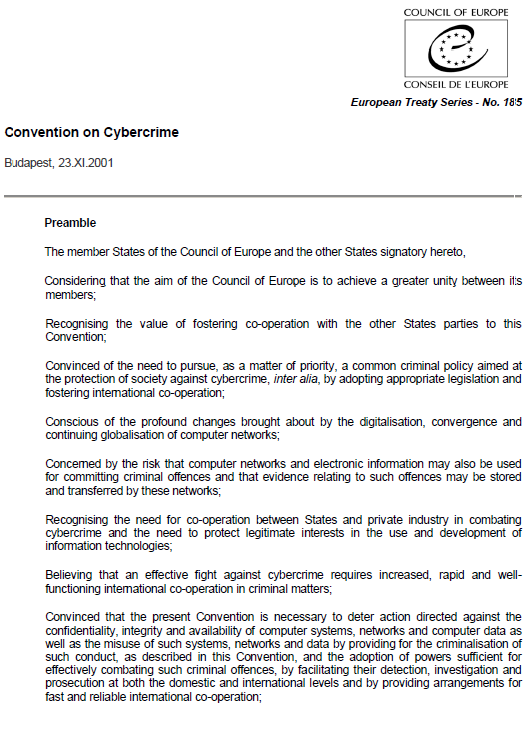
Указ Президента «Про Положення про Сили спеціальних операцій Збройних Сил України» 25.02. 2017 р.

Укази Президента України: від 26.05.2015р.№ 287/2015/ «Про рішення РНБО України від 6.05. 2015 р. «Про Стратегію національної безпеки України»»

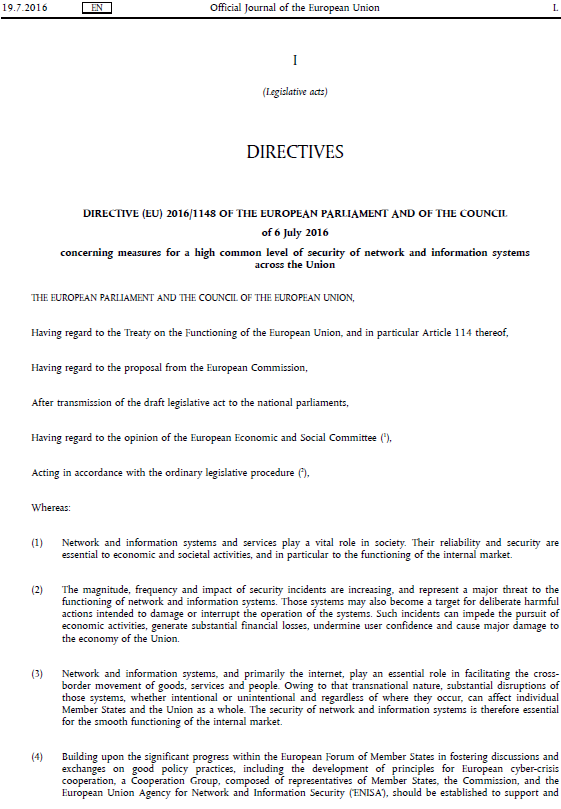
від 14.03.2016 р. № 92/2016 «Про рішення РНБО України від 4.03.2016 р. «Про Концепцію розвитку сектору безпеки і оборони України»»

Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

2.4 Міжнародні акти, що закріплюють стандарти запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку



|  |  |
| --- | --- |
| **Конвенція  про кіберзлочинність**  (Додатковий протокол від 28.01.2003 до Конвенції)  (Конвенцію ратифіковано із застереженнями і заявами Законом від 07.09.2005. ВВР. 2006. № 5-6. Ст.71)  Дата підписання: 23.11.2001  Дата ратифікації: 07.09.2005  Дата набрання чинності: 01.07.2006 | |
| Preamble  The member States of the Council of Europe and the other States signatory hereto,  Considering that the aim of the Council of Europe is to achieve a greater unity between its members;  Recognising the value of fostering co-operation with the other States parties to thisConvention;  Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;  Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;  Concerned by the risk that computer networks and electronic information may also be used  for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;  Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;  Believing that an effective fight against cybercrime requires increased, rapid and wellfunctioning international co-operation in criminal matters; | Преамбула  Держави-члени Ради Європи та інші Держави, які підписали цю Конвенцію,  Вважаючи, що метою Ради Європи є досягнення більшої єдності між її членами;  Визнаючи цінність налагодження співробітництва з іншими Державами, які є Сторонами цієї Конвенції;  Впевнені у першочерговій необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва;  Усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, яка продовжується;  Стурбовані ризиком того, що комп'ютерні мережі та електронна інформація може також використовуватися для здійснення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами;  Визнаючи необхідність співробітництва між Державами і приватними підприємствами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів у ході використання і розвитку інформаційних технологій;  Вважаючи, що ефективна боротьба з кіберзлочинністю вимагає більшого, швидкого і ефективно функціонуючого міжнародного співробітництва у кримінальних питаннях; |
| **Chapter II** Measures to be taken at the national level  **Section 1 Substantive criminal law**  **Title 1 Offences against the confidentiality, integrity and availability of computer data and systems**  **Article 2 Illegal access**  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.  **Article 3 Illegal interception**  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.  **Article 4 – Data interference**  1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.  2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.  **Article 5 – System interference**  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious  hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.  **Article 6 – Misuse of devices**  1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:  a the production, sale, procurement for use, import, distribution or otherwise making available of:  i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;  ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and  b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.  2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.  3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.  **Title 2 – Computer-related offences**  **Article 7 Computer-related forgery**  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an  intent to defraud, or similar dishonest intent, before criminal liability attaches.  **Article 8 – Computer-related fraud**  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:  a. any input, alteration, deletion or suppression of computer data,  b. any interference with the functioning of a computer system,  with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself  or for another person.  **Title 3 Content-related offences**  **Article 9** Offences related to child pornography  1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:  a. producing child pornography for the purpose of its distribution through a computer system;  b. offering or making available child pornography through a computer system;  c. distributing or transmitting child pornography through a computer system;  d. procuring child pornography through a computer system for oneself or for another person;  e. possessing child pornography in a computer system or on a computer-data storage medium.  2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:  a. a minor engaged in sexually explicit conduct;  b. a person appearing to be a minor engaged in sexually explicit conduct;  c. realistic images representing a minor engaged in sexually explicit conduct.  3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than  16 years.  4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.  **Title 4 Offences related to infringements of copyright and related rights**  **Article 10** Offences related to infringements of copyright and related rights  1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.  2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.  3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article. | **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, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, 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 (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, 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. |
| **Section 2 – Procedural law**  *Title 1 – Common provisions*  **Article 14 – Scope of procedural provisions**  1. Each Party shall adopt such legislative and other measures as may be necessary to establishthe powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.  2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:  a. the criminal offences established in accordance with Articles 2 through 11 of thisConvention;  b. other criminal offences committed by means of a computer system; and  c. the collection of evidence in electronic form of a criminal offence.  3.a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of  such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider  restricting such a reservation to enable the broadest application of the measure referred to in Article 20.  b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20  and 21 to communications being transmitted within a computer system of a service provider, which system:  i. is being operated for the benefit of a closed group of users, and  ii. does not employ public communications networks and is not connected with another computer system, whether public or private,  that Party may reserve the right not to apply these measures to such сommunications.  Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.  **Article 15** Conditions and safeguards  1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental  Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.  2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.  3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties. | **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., Міжнародною Хартією ООН про  громадянські і політичні права 1966 р., 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. |
| **Article 16 –** Expedited preservation of stored computer data | **Стаття 16** - Термінове збереження комп'ютерних даних, які зберігаються |
| **Article 17 –** Expedited preservation and partial disclosure of traffic data | **Стаття 17** - Термінове збереження і часткове розкриття даних про рух інформації |
| **Title 3 Production order**  **Article 18** – Production order | **Заголовок 3 Порядок представлення**  **Стаття 18** Порядок представлення |
| **Title 4 – Search and seizure of stored computer data**  Article 19 – Search and seizure of stored computer data | **Заголовок 4 - Обшук і арешт комп'ютерних даних, які зберігаються**  Стаття 19 - Обшук і арешт комп'ютерних даних, які берігаються |
| **Title 5 – Real-time collection of computer data**  **Article 20 –** Real-time collection of traffic data | **Заголовок 5 Збирання комп'ютерних даних у реальному масштабі часу**  **Стаття 20** - Збирання даних про рух інформації у реальному масштабі часу |
| **Article 21** – Interception of content data | **Стаття 21** - Перехоплення даних змісту інформації |
| **Section 3 –** Jurisdiction  **Article 22 –** Jurisdiction | Частина 3 - Юрисдикція  **Стаття 22** - Юрисдикція |
| **Chapter III – International co-operation**  **Section 1 – General principles**  Title 1 – General principles relating to international co-operation  **Article 23** – General principles relating to international co-operation | **Розділ III** - **Міжнародне співробітництво**  **Частина 1 - Загальні принципи**  Заголовок 1 - Загальні принципи   міжнародного співробітництва  **Стаття 23** - Загальні принципи   міжнародного співробітництва |
| Title 2 Principles relating to xtradition  **Article 24 –** Extradition | **Заголовок 2 Принципи екстрадиції**  **Стаття 24** - Екстрадиція |
| **Title 3 – General principles relating to mutual assistance**  **Article 25 –** General principles relating to mutual assistance  1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.  2. Each Party shall also adopt such legislative and other measures as may be necessary to  carry out the obligations set forth in Articles 27 through 35.  3. Each Party may, in urgent circumstances, make requests for mutual assistance or  communications related thereto by expedited means of communication, including fax or email,  to the extent that such means provide appropriate levels of security and authentication  (including the use of encryption, where necessary), with formal confirmation to follow, where  required by the requested Party. The requested Party shall accept and respond to the request  by any such expedited means of communication.  4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse coope-ration. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it onsiders a fiscal offence.  5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. | **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 право-порушень, пов'язаних з комп'ю-терними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального право-порушення.  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 (включа-ючи 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 запи-тують, або до відповідних договорів про взаємну допомогу, включаючи підстави, на яких Сторона, яку запитують, може відмовити у співробітництві. Сторона, яку запи-тують, 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 правопо-рушення, 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 правопо-рушення, стосовно якого запитується допомога, є кримінальним правопо-рушенням відповідно до законо-давства Сторони, яку запитують. |
| **Article 26** – Spontaneous information  1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying  out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.  2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. | **Стаття 26** - Добровільно надана інформація  1. Сторона може в рамках свого зако-нодавства без попереднього запиту надіслати іншій Стороні інформацію, отриману в ході її власного роз-слідування, якщо вона вважає, що розкриття такої інформації може допомогти Стороні, яка отримує інформацію, у відкритті або прове-денні розслідування чи переслі-дування 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 використо-вувалася 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. |
| **Article 27 – Procedures pertaining to mutual assistance requests in the absence of**  **applicable international agreements**  1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. | **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 законо-давства, якщо тільки заінтересовані Сторони не погоджуються застосо-вувати замість них, частково або повністю, нижчевикладені положення цієї статті. |
| **Article 28 – Confidentiality and limitation on use**  2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:  a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or  b. not used for investigations or proceedings other than those stated in the request. | **Стаття 28** - Конфіденційність і обмеження у використанні  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. |
| **Section 2 – Specific provisions**  Title 1 – Mutual assistance regarding provisional measures  **Article 29 –** Expedited preservation of stored computer data  1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. | **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. |
| **Article 30 –** Expedited disclosure of preserved traffic data  1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of  traffic data to identify that service provider and the path through which the communication was transmitted.  2. Disclosure of traffic data under paragraph 1 may only be withheld if:  a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or  b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. | **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. |
| **Title 2** – Mutual assistance regarding investigative powers  **Article 31** – Mutual assistance regarding accessing of stored computer data  1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. | **Заголовок 2 -** Взаємна допомога щодо повноважень на 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 збері-гаються за допомогою комп'ю-терної системи, яка знаходиться на території Сторони, яку запитують, включаючи дані, збережені відповідно до статті 29. |
| **Article 32 –** Trans-border access to stored computer data with consent or where publicly available | **Стаття 32** - Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними |
| **Article 33** – Mutual assistance regarding the real-time collection of traffic data | **Стаття 33** - Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу |
| **Article 34 –** Mutual assistance regarding the interception of content data  The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws. | **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 відпо-відними договорами між ними і вну-трішньодержавним законодавством. |
| **Title 3 – 24/7 Network**  **Article 35** – 24/7 Network  1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-aweek basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:  a. the provision of technical advice;  b. the preservation of data pursuant to Articles 29 and 30;  c. the collection of evidence, the provision of legal information, and locating of suspects. | **Заголовок 3 - Цілодобова мережа**  **Стаття 35** - Цілодобова мережа  1. Кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання не-гайної допомоги для розслідування або переслідування стосовно кримі-нальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрі-шньодержавним законодавством і  практикою, пряме:  a. надання технічних порад;  b. збереження даних відповідно до статей 29 і 30; та  c. збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних. |



|  |
| --- |
| Директива (EU) 2015/849 Європейського Парламенту та Ради від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, що вносить зміни до Регламенту (EU) № 648/2012 Європейського Парламенту і Ради, а також скасовує Директиву 2005/60/ЕС Європейського Парламенту і Ради та Директиву Комісії 2006/70/ЕС  (Текст доречний для Європейського Економічного Простору (ЄЕП)) |
| ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ ТА РАДА ЄВРОПЕЙСЬКОГО СПІВТОВАРИСТВА,  Ураховуючи, що:   |  |  | | --- | --- | | (3) | Дана Директива є четвертою Директивою, яка спрямована на запобігання загрози відмивання грошей. Директива Ради 91/308/EEC визначала відмивання грошей з точки зору правопорушень, пов’язаних з наркотиками, і накладала зобов'язання виключно на фінансовий сектор. Директива 2001/97/EC Європейського Парламенту та Ради розширила сферу дій Директиви 91/308/EEC як з точки зору охоплення злочинів, так і з точки зору охоплення сукупності професій та видів діяльності. У червні 2003 року, Група розробки фінансових заходів боротьби з відмиванням грошей (FATF) переглянула свої рекомендації, щоб охопити фінансування тероризму, та надала більш детальні вимоги стосовно ідентифікації клієнта та перевірки, ситуацій, в яких більш високий ризик відмивання грошей або фінансування тероризму може виправдати підвищені заходи, а також ситуації, в яких знижений рівень ризику може виправдати менш суворий контроль. Зазначені зміни були відображені в Директиві 2005/60/EC Європейського Парламенту та Ради та в Директиві Комісії 2006/70/EC. |  |  |  | | --- | --- | | (4) | Відмивання грошей та фінансування тероризму часто здійснюються в міжнародному контексті. Заходи, вжиті виключно на національному або навіть на рівні Союзу, без урахування міжнародного співробітництва та координації, будуть мати дуже обмежений результат. Таким чином заходи, прийняті Союзом в зазначеній сфері, повинні бути сумісними з, та принаймні, настільки ж строгими, як, інші заходи, що вживаються на міжнародному рівні. Діяльність Союзу повинна продовжувати приділяти особливу увагу Рекомендаціям FATF та інструментам інших міжнародних органів, що діють у боротьбі з відмиванням грошей і фінансуванням тероризму. З метою посилення ефективності боротьби з відмиванням грошей і фінансуванням тероризму, відповідні нормативно-правові акти Союзу повинні, у доречних випадках, бути приведені у відповідність з міжнародними стандартами по боротьбі з відмиванням грошей і фінансуванням тероризму та його розповсюдженням, прийнятими FATF у лютому 2012 року («оновлені Рекомендації FATF»). |  |  |  | | --- | --- | | (6) | Використання великих грошових платежів є дуже уразливим для відмивання грошей та фінансування тероризму. З метою збільшення настороженості та зниження ризиків, виникнення яких пов'язане з такими грошовими виплатами, на особистостей, які здійснюють торгівлю товарами, повинні поширюватись положення даної Директиви за умови, що вони здійснюють або отримують грошові виплати в розмірі 10000 євро або більше. |  |  |  | | --- | --- | | (7) | Використання електронних грошових продуктів все частіше розглядається в якості заміни для банківських рахунків, що крім заходів, викладених в Директиві 2009/110/EC Європейського Парламенту та Ради, обґрунтовує, що на зазначені продукти поширюються зобов’язання по боротьбі з відмиванням грошей і протидії фінансуванню тероризму (БВГ/ПФТ) зобов'язань. |  |  |  |  | | --- | --- | --- | | (18) |  | Положення даної Директиви повинні також застосовуватись до діяльності зобов’язаних суб’єктів, які здійснюється в мережі інтернет. | | (56) |  | Удосконалення обміну інформацією між FIU в рамках Союзу є особливо важливим у процесі вирішення проблеми транснаціонального характеру відмивання грошей і фінансування тероризму. Використання надійних механізмів для обміну інформацією, зокрема децентралізованої комп'ютерної мережі FIU.net («FIU.net») або її наступних варіантів і методів, запропонованих FIU.net, повинне заохочуватись державами-членами. Початковий обмін інформацією між FIU, що відноситься до відмивання грошей або фінансування тероризму, для аналітичних цілей, які надалі не обробляються або не розповсюджуються, має бути дозволений, якщо такий обмін інформацією не суперечив би основним принципам національного законодавства. Обмін інформацією про випадки, визначені FIU, як такі, що можливі із залученням податкових злочинів, повинен здійснюватися без шкоди для обміну інформацією в сфері оподаткування відповідно до положень Директиви Ради 2011/16/EU [(15)](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849#ntr15-L_2015141EN.01007301-E0015) або відповідно до міжнародних стандартів з обміну інформацією та адміністративного співробітництва в податкових питаннях. |  |  |  | | --- | --- | | (57) | Для того, щоб мати можливість повною мірою і оперативно реагувати на запити FIU, зобов'язані особи повинні мати ефективні системи, які дозволяють їм мати повний і своєчасний доступ через безпечні і конфіденційні канали до інформації про ділові відносин, які вони підтримують або зберегли з зазначеними персонами. Відповідно до законодавства Союзу і національних законодавств держави-члени могли б, наприклад, розглядати питання про запровадження систем банківських реєстрів або електронних систем вилучення даних, які забезпечили б FIU доступ до інформації про банківські рахунки без шкоди для судової влади у випадках, в яких це може бути застосовано. Держави-члени могли б також розглянути питання про створення механізмів для забезпечення того, щоб компетентні органи мають процедури для ідентифікації активів без попереднього повідомлення власника. |  |  |  | | --- | --- | | (58) | Держави-члени повинні заохочувати свої компетентні органи надавати швидко, конструктивно і ефективно широкий спектр транскордонного співробітництва для цілей цієї Директиви без шкоди для будь-яких правил або процедур, які можна застосувати до судової співпраці у кримінальних справах. Держави-члени повинні, зокрема, забезпечити, щоб їх FIU обмінювались інформацією вільно, спонтанно або за запитом, з підрозділами фінансової розвідки третіх країн, беручи до уваги права Союзу і принципи в сфері обміну інформацією, розроблені Егмонтською групою підрозділів фінансової розвідки. | |

2.5 Зміст міжнародних стандартів з запобігання злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

|  |
| --- |
| **ДИРЕКТИВА (ЄС) 2016/1148 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ**  **від 6 липня 2016 року**  **щодо заходів щодо високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі** |
| |  |  | | --- | --- | | (4) | Спираючись на значний прогрес у рамках Європейського форуму держав-членів у сприянні дискусіям та обміну передовою політичною практикою, включаючи розробку принципів європейського співробітництва в галузі кіберкризи, Група співпраці, що складається з представників держав-членів, Комісії та Слід **створити Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA)** для підтримки та сприяння стратегічному співробітництву між державами-членами щодо безпеки мережі та інформаційних систем. Для того, щоб ця група була ефективною та інклюзивною, важливо, щоб усі держави-члени мали мінімальні можливості та стратегію, що забезпечує високий рівень безпеки мережевих та інформаційних систем на своїй території. | |
| |  |  | | --- | --- | | (18) | Функція пункту обміну Інтернетом (IXP) полягає у взаємозв'язку мереж. IXP не надає доступу до мережі або виступає транзитним постачальником або перевізником. Також IXP не надає інших послуг, не пов’язаних із взаємозв’язком, хоча це не заважає оператору IXP надавати не пов’язані між собою послуги. **IXP існує для взаємозв'язку мереж**, які технічно та організаційно відокремлені. Термін "автономна система" використовується для опису технічно автономної мережі. | |
| |  |  | | --- | --- | | (32) | Компетентні органи влади або **групи реагування на випадки комп’ютерної безпеки** **(далі - CSIRT)** повинні отримувати повідомлення про інциденти. Єдині контактні пункти не повинні отримувати безпосередньо будь-яких повідомлень про інциденти, якщо вони також не виступають як компетентний орган або CSIRT. Однак компетентний орган або CSIRT повинні мати змогу доручити єдиному контактному пункту передавати повідомлення про події до єдиних контактних пунктів інших постраждалих держав-членів. | |
| |  |  | | --- | --- | | (34) | Держави-члени повинні бути належним чином оснащені як технічними, так і організаційними можливостями для запобігання, виявлення, реагування та пом'якшення інцидентів та ризиків у мережі та інформаційній системі. Отже, **держави-члени повинні забезпечити наявність у них добре функціонуючих CSIRT**, також відомих як комп’ютерні команди реагування на надзвичайні ситуації (CERT), які відповідають основним вимогам, щоб гарантувати ефективні та сумісні можливості для вирішення інцидентів та ризиків та забезпечення ефективної співпраці на рівні Союзу. Для того, щоб усі типи операторів основних послуг та постачальники цифрових послуг могли скористатися такими можливостями та співпрацею, держави-члени повинні забезпечити, щоб усі типи охоплювались спеціальним CSIRT. Враховуючи важливість міжнародного співробітництва у галузі кібербезпеки, | |
| |  |  | | --- | --- | | (35) | Оскільки більшість мережевих та інформаційних систем працюють приватно, **співпраця між державним та приватним секторами є надзвичайно важливою**. Операторів основних послуг та постачальників цифрових послуг слід заохочувати застосовувати власні механізми неформальної співпраці для забезпечення безпеки мережі та інформаційних систем. Група співпраці повинна мати можливість запрошувати відповідних зацікавлених сторін на обговорення, де це доречно. Щоб ефективно заохочувати обмін інформацією та передовою практикою, важливо забезпечити, щоб оператори основних послуг та постачальники цифрових послуг, які беруть участь у таких обмінах, не зазнали збитків у результаті їх співпраці. | |
| |  |  | | --- | --- | | (36) | **ENISA повинна допомагати державам-членам та Комісії, надаючи досвід та поради та сприяючи обміну передовою практикою**. Зокрема, при застосуванні цієї Директиви Комісія повинна, а держави-члени повинні мати можливість консультуватися з ENISA. Для зміцнення потенціалу та знань серед держав-членів Група співпраці повинна також слугувати інструментом для обміну передовою практикою, обговорення можливостей та готовності держав-членів, а також на добровільній основі допомагати своїм членам в оцінці національних стратегій щодо безпека мережевих та інформаційних систем, нарощування потенціалу та оцінка вправ, що стосуються безпеки мережевих та інформаційних систем. |  |  |  | | --- | --- | | (37) | За необхідності, держави-члени повинні мати можливість **використовувати** або адаптувати **існуючі організаційні структури** або стратегії при застосуванні цієї Директиви. | |
| |  |  | | --- | --- | | (39) | З метою сприяння вдосконаленій безпеці мережевих та інформаційних систем **Група співробітництва повинна, де це доречно, співпрацювати з відповідними установами**, органами, офісами та установами Союзу, обмінюватися ноу-хау та передовою практикою та надавати поради щодо аспектів безпеки мережі. та інформаційні системи, які можуть вплинути на їх роботу, дотримуючись існуючих механізмів обміну обмеженою інформацією. Співпрацюючи з правоохоронними органами щодо аспектів безпеки мережі та інформаційних систем, які можуть вплинути на їх роботу, Група співробітництва повинна поважати існуючі канали інформації та створені мережі. | |
| |  |  | | --- | --- | | (41) | **Якщо інформація вважається конфіденційною** відповідно до правил Союзу та національних правил щодо ділової конфіденційності, така **конфіденційність повинна забезпечуватися** під час здійснення діяльності та виконання цілей, встановлених цією Директивою. | |
| |  |  | | --- | --- | | (42) | **Вправи, що імітують сценарії інцидентів у реальному часі, є надзвичайно важливими для перевірки готовності та співпраці** держав-членів щодо безпеки мережевих та інформаційних систем. Цикл навчань CyberEurope, координований ENISA за участю держав-членів, є корисним інструментом для тестування та складання рекомендацій щодо того, як з часом покращуватись обробка інцидентів на рівні Союзу. Враховуючи, що в даний час держави-члени не зобов'язані ні планувати, ні брати участь у навчаннях, створення мережі CSIRT відповідно до цієї Директиви повинно дозволити державам-членам брати участь у навчаннях на основі точного планування та стратегічного вибору. Група співпраці, створена відповідно до цієї Директиви, повинна обговорити стратегічні рішення щодо навчань, зокрема, але не виключно щодо регулярності навчань та розробки сценаріїв. ENISA повинна, відповідно до свого мандату, підтримувати організацію та проведення загальносоюзних навчань, надаючи свої знання та поради Групі співробітництва та мережі CSIRT. | |
| |  |  | | --- | --- | | (43) | З огляду на глобальний характер проблем безпеки, що зачіпають мережеві та інформаційні системи, існує **потреба у більш тісному міжнародному співробітництві** з метою вдосконалення стандартів безпеки та обміну інформацією та сприяння загальному глобальному підходу до питань безпеки. | |
| |  |  | | --- | --- | | (49) | **Постачальники цифрових послуг повинні забезпечувати рівень безпеки, відповідний ступеню ризику для безпеки цифрових послуг, які вони надають, з огляду на важливість їхніх послуг для діяльності інших підприємств у межах Союзу.** На практиці ступінь ризику для операторів основних послуг, які часто необхідні для підтримки критичної соціальної та економічної діяльності, вища, ніж для постачальників цифрових послуг. Отже, вимоги до безпеки постачальників цифрових послуг повинні бути меншими. Постачальники цифрових послуг повинні залишатися вільними вживати заходів, які, на їх думку, є доцільними для управління ризиками, пов'язаними з безпекою їх мережі та інформаційних систем. Через їх транскордонний характер, постачальники цифрових послуг повинні застосовувати більш гармонізований підхід на рівні Союзу. | |
| |  |  | | --- | --- | | (52) | **Оператори основних послуг та постачальники цифрових послуг повинні забезпечувати безпеку мережі та інформаційних систем**, якими вони користуються. Це, в першу чергу, приватні мережеві та інформаційні системи, якими керує їхній внутрішній ІТ-персонал, або безпека яких була передана на підряд. Вимоги щодо безпеки та сповіщення повинні поширюватися на відповідних операторів основних послуг та постачальників цифрових послуг, незалежно від того, виконують вони внутрішнє технічне обслуговування своєї мережі та інформаційних систем або передають їх на роботу стороннім постачальникам. | |
| |  |  | | --- | --- | | (56) | Ця **Директива не повинна перешкоджати** державам-членам приймати **національні заходи**, що вимагають від органів державного сектору забезпечувати конкретні вимоги безпеки, коли вони укладають послуги хмарних обчислень. Будь-які такі національні заходи повинні застосовуватися до відповідного органу державного сектору, а не до постачальника послуг хмарних обчислень. | |
| |  |  | | --- | --- | | (60) | **Постачальники цифрових послуг повинні підлягати легкому дотику та реактивній *постнаглядовій* діяльності**, обґрунтованій характером своїх послуг та операцій. | |
| |  |  | | --- | --- | | (61) | Компетентні органи повинні мати необхідні засоби для виконання своїх обов'язків, включаючи повноваження щодо отримання достатньої інформації для оцінки рівня безпеки мережі та інформаційних систем. | |
| |  |  | | --- | --- | | (62) | Інциденти можуть бути наслідком злочинної діяльності, запобігання, розслідування та переслідування якої підтримується координацією та співпрацею між операторами основних послуг, постачальниками цифрових послуг, компетентними органами та правоохоронними органами. Якщо є підозра, що інцидент пов’язаний із серйозною злочинною діяльністю згідно із законодавством Союзу або національним законодавством, держави-члени повинні заохочувати операторів основних послуг та постачальників цифрових послуг повідомляти відповідні правоохоронні органи про випадки підозри у серйозному кримінальному характері. За необхідності **бажано, щоб координація між компетентними органами та правоохоронними органами різних держав-членів сприяла Європейському центру з кіберзлочинності (EC3) та ENISA.** | |
| |  |  | | --- | --- | | (66) | **Стандартизація вимог безпеки** - це ринковий процес. Для забезпечення конвергентного застосування стандартів безпеки держави-члени повинні заохочувати дотримання або відповідність зазначеним стандартам, щоб забезпечити високий рівень безпеки мережевих та інформаційних систем на рівні Союзу. ENISA повинна допомагати державам-членам через поради та рекомендації. З цією метою може бути корисним скласти гармонізовані стандарти, які слід робити відповідно до Регламенту (ЄС) No 1025/2012 Європейського Парламенту та Ради | |
| |  |  | | --- | --- | | (72) | **Обмін інформацією про ризики та інциденти в рамках Групи співпраці та мережі CSIRT та дотримання вимог щодо повідомлення національних компетентних органів або CSIRT про інциденти може зажадати обробки персональних даних.** Така обробка повинна відповідати Директиві 95/46 / ЄС Європейського Парламенту та Ради та Регламенту (ЄС) No 45/2001 Європейського Парламенту та Ради. При застосуванні цієї Директиви слід застосовувати Регламент (ЄС) No 1049/2001 Європейського Парламенту та Ради, якщо це доречно | |

**Стандарти запобігання кіберзлочинам згідно Посібника Комітету ООН з запобігання кіберзлочинам**

1. Співробітництво у боротьбі з комп’ютерною злочинністю має розвиватися та вдосконалюватися на рівнях

національному

На національному рівні можуть бути створені робочі групи для вирішення відповідних питань. Ці групи можуть залучати своїх членів з різних дисциплін та галузей, включаючи уряд, промисловість та наукові спільноти

вивчення досвіду, набутого в цій галузі, включаючи матеріали, викладені в Посібнику, та проведення аналізу своїх національних ситуацій та законів

розгляд можливість прийняття заходів:

Перегляд стану законодавства у світлі питань, порушених у Посібнику, оцінка матеріальної та процесуальної адекватності їх правової та адміністративної інфраструктури та рекомендація відповідних рішень

міжнародному

Проведення огляду законодавства, політики та практики призначення покарань з метою розробки більш ефективних положень щодо покарання у сфері покарання.

**Стандарти запобігання кіберзлочинам згідно Посібника Комітету ООН з запобігання кіберзлочинам**

3. Міжнародне співробітництво у сфері реформування покарань забезпечило б рівномірне ставлення до злочинців, пов’язаних із комп’ютерною злочинністю, і могло б перешкодити переселенню комп’ютерних правопорушників до юрисдикцій, де зловживання комп’ютером могло б ставитися м’якше

4. Забезпечення періодичних оглядів та реформування законів, політики та практики з метою врахування змін, що виникають внаслідок технологічних розробок та тенденцій в галузі комп’ютерної злочинності

5. Запрошення навчальних закладів, асоціацій виробників апаратного та програмного забезпечення та галузі обробки даних додати курси з правових та етичних аспектів комп'ютерів до своїх навчальних програм та навчальних програм з метою запобігання зловживанню комп'ютерами та створення етичних стандартів для відповідних секторів

6. Розробка механізму навчання потенційних жертв комп’ютерних злочинів та викриття реальних масштабів комп’ютерних злочинів. Слід заохочувати активну участь жертв у розробці програм профілактики та програм допомоги жертвам, які пропорційні масштабу проблеми

2. Співпраця в обміні досвідом та інформацією про законодавство та судові та правоохоронні процедури, що застосовуються до комп’ютерних злочинів

**Стандарти запобігання кіберзлочинам згідно Посібника Комітету ООН з запобігання кіберзлочинам**

8. Консультування з групами в інших країнах та з метою не відставати від досягнень сучасних комп’ютерних злочинів, консолідація та сприяння зусиллям правоохоронних органів, включаючи розробку та навчання інноваційним методам для слідчого та прокурорського персоналу

9. Впровадження добровільних заходів безпеки користувачами комп’ютерів у приватному секторі

10. Введення обов’язкових заходів безпеки в певних делікатних секторах

7. З огляду на міжнародний характер обробки даних та інформаційних технологій, розподіл стандартів безпеки та процедурних методів між усіма галузями галузі, як на національному, так і на міжнародному рівні

11. Заохочення створення та імплементації національного законодавства, політики та керівних принципів комп’ютерної безпеки

**Стандарти запобігання кіберзлочинам згідно Посібника Комітету ООН з запобігання кіберзлочинам**

15. Розробка професійних стандартів у галузі обробки даних, включаючи можливість застосування дисциплінарних заходів

16. Навчання громадськості щодо поширеності комп’ютерної злочинності та необхідності пропаганди комп’ютерної етики, стандартів та заходів безпеки

17. Сприяння співпраці жертв у повідомленні про комп’ютерні злочини

18. Навчання та виховання персоналу у слідчій, прокурорській та судовій системах

14. Розвиток та просування комп’ютерної етики у всіх секторах суспільства, але особливо в освітніх закладах та професійних товариствах

13. Включення та сприяння використанню заходів безпеки в галузі інформаційних технологій

12. Заохочення керівництва та керівників вищих рівнів привертати свої організації до безпеки та попередження злочинів

Правовий вимір вирішення проблем запобігання злочинам у сфері сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

|  |
| --- |
| Організаційний вимір |
| Розуміння принципів управління безпекою ІКТ, зокрема щодо наступних тем: |
| x Оцінка вразливостей та загроз;  x Місія безпеки, практика управління та умови успіху;  x Як визначити цінні активи та пов'язані з ними ризики;  x Як визначити політику безпеки;  x Як організувати місію безпеки, контролювати, оцінювати, проводити аудит, оцінювати вартість;  x Як керувати безпекою в складних та динамічних середовищах. |
| Мета: організація можливостей: |
| x Створити ефективний процес безпеки та освоїти пов'язані з ІКТ ризики та витрати на безпеку;  x Співпрацювати з юридичними, правоохоронними та технічними працівниками;  x Створити відповідні організаційні структури та процедури. |
| Технологічний вимір |
| Щодо технологічного виміру кібербезпеки, професіоналам ІКТ слід: |
| x розуміти технічні вразливості та неправильне використання ІКТ;  x розуміти ризики, пов'язані з ІКТ, кіберзагрози та кібератаки;  x Розуміти суспільні та організаційні проблеми та цінності. |
| Для можливостей: |
| x Зменшити кількість вразливостей цифрових середовищ;  x Визначити, спроектувати, виготовити та впровадити ефективні засоби безпеки та заходи захисту та реагування на підтримку доступності, цілісності та конфіденційності інфраструктури ІКТ та формування довіри до електронних послуг. |
| Технології безпеки повинні бути: |
| x Економічно вигідні;  x Зручні для користувача;  x Прозорі;  x Аудиторські;  x Контрольовані сторонньою стороною. |
| Міжнародний підхід |
| прийняття міжнародних стандартів та передової практики у всіх аспектах кібербезпеки. |
| Універсальний підхід до інформаційної безпеки корисний для: |
| x Мати загальне розуміння того, що кібербезпека означає для всіх;  x Сприяти формуванню глобальної реакції на безпечне та взаємопов’язане інформаційне суспільство;  x Сприяти визначенню та розгортанню національних стратегій кібербезпеки та міжнародної співпраці;  x Створювати місцеві ноу-хау на основі загальновизнаних стандартів, щоб відповідати конкретним місцевим потребам шляхом інтеграції місцевих культурних цінностей у національні стандарти, що походять від міжнародних стандартів та добре визнаної доброї практики;  x Уникати дублювання робіт та зусиль;  x Оптимізувати співпрацю між учасниками;  х Однакове застосування міжнародних стандартів |
| Вирішення глобальних питань |
| x Належне використання ІКТ;  x Технічні заходи;  x Економічні, правові та політичні питання;  х Вироблення культури кібербезпеки для належного розуміння стандартів кожним членом ланцюга кібербезпеки. |
| Мета застосування заходів запобігання кіберзлочинам |
| Звичайні заходи запобігання політики безпеки полягають у підвищенні загального рівня ризику для злочинців та в зменшенні вигідних очікувань. Це передбачає спроможність виявляти діяльність злочинців через Інтернет, локалізувати, ідентифікувати та переслідувати їх. |
| Заходи запобігання кіберзлочинам |
| Заходи, передбачені **Конвенцією про кіберзлочинність**  Стаття 15 - Умови і запобіжні заходи  Стаття 16 - Термінове збереження комп'ютерних даних, які зберігаються  Стаття 17 - Термінове збереження і часткове розкриття даних про рух інформації  Стаття 18 - Порядок представлення  Стаття 19 - Обшук і арешт комп'ютерних даних, які зберігаються  Стаття 20 - Збирання даних про рух інформації у реальному масштабі часу  Стаття 21 - Перехоплення даних змісту інформації  Стаття 23 - Загальні принципи міжнародного співробітництва |
| Глобальні проблеми |
| x Глобальна та добре зрозуміла культура кібербезпеки для всіх суб’єктів інформаційного суспільства;  x Адекватні правові, організаційні та технічні заходи;  x Міжнародне співробітництво для боротьби з кіберзлочинністю та забезпечення безпеки інфраструктур ІКТ. |

2.6 Основні проблеми протидії злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

2.7 Кіберзагрози національній безпеці України та запобігання їм

**Нормативно-правовий та інституційний базис**

**кібербезпеки в ЄС, НАТО й Україні**

* 2001 р. Європейська Комісія: Комунікація «Безпека мережі та інформації» (Network and Information Security (NIS): Proposal for A European Policy Approach)
* 2006 ЄС: схвалена Стратегія безпечного інформаційного суспільства (Strategy for a Secure Information Society)
* 2009 р. ЄС схвалена Комунікація «Захист критичної інформаційної інфраструктури» (Communication on Critical Information Infrastructure Protection, CIIP)
* 2012 р. в ЄС створена Група з питань реагування на інциденти в галузі комп’ютерної безпеки (Computer Emergency Response Team, CERT-EU)
* 2013 р. ЄС: схвалено Кібер-стратегію ЄС.
* 2016 р. ЄС схвадено Глобальна стратегія із зовнішньої і безпекововї політики ЄС (Кібер-стратегія ЄС «Відкритий, надійний і безпечний кіберпростір» (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)
* 2016 р. ЄС : Директива з безпеки мереж та інформаційних систем (NIS directive - Directive (EU) 2016/1148):
* кіберстійкість, зменшення кіберзлочинності, розвиток можливостей і політики кіберзахисту, індустріальних і технологічних ресурсів кібербезпеки, послідовної міжнародної політики з кіберпростору
* 2017 р. ЄС доповнив Стратегію «Спільною комунікацією Європейської служби зовнішньої дії і Єврокомісії з розбудови належної кібербезпеки ЄС» - посилення Агентства кібербезпеки ЄС (ENISA)

**Нормативно-правовий та інституційний базис**

**кібербезпеки в ЄС, НАТО й Україні**

* 2017 р. в ЄС запущено Постійне Структуроване Співробітництво (Permanent Structured Cooperation on Defence, PESCO)
* створення Груп швидкого реагування на кіберзагрози (Cyber Rapid Response Teams).
* Позитивне для України: треті країни можуть запрошуватись до участі в окремих проектах PESCO, включаючи сферу кіберзахисту.
* 2018 р. Європейський Парламент, Європейська Рада і Європейська Комісія досягли політичної згоди щодо Акту з кібербезпеки (Cybersecurity Act), який також посилює мандат Європейського Агентства Мережевої та Інформаційної Безпеки (European Network and Information Security Agency (ENISA) + встановлює рамки для сертифікації з кібербезпеки, прискорює розвиток онлайн сервісів з кібербезпеки.
* 2017 Єврокомісія запропонувала створити Фонд реагування на надзвичайні ситуації з кібербезпеки (Cybersecurity Emergency Response Fund)
* 2018 р. Єврокомісія схвалила рішення про створення мережі центрів компетентності в країнах-членах за координації Європейського центру досліджень і компетентності з кібербезпеки
* створена Європейська платформа публічно-приватного партнерства стійкості (European Public-Private Partnership for Resilience)

|  |
| --- |
| **Агентства ЄС з питань кібербезпеки** |
| В Агентстві Європол діє Європейський Центр протидії кібер-злочинності (European Cybercrime Centre, EC3) |
| Євроюст (Eurojust) |
| Європейський поліцейський коледж |
| Європейська служба зовнішньої дії |
| Європейське оборонне агентство(EDA) |



|  |
| --- |
| **НАТО** |
| На Уельському саміті 2014 року НАТО схвалив посилену політику з кібероборони і відповідний план дій з її імплементації |
| На Варшавському саміті 2016 року Альянс вже зосередив увагу на посиленні кібероборони національних мереж та промисловості. Тоді ж був підтверджений мандат НАТО на проведення операцій у кіберпросторі, який прирівняли до інших сфер проведення операцій – суші, повітря і моря |
| На Брюссельському саміті НАТО 2018 року кібератаки віднесені до головних гібридних загроз.  НАТО погодило необхідність доведення операцій з кібероборони до рівня операцій в інших трьох сферах як за загальної координації Альянсу, так і в межах окремих груп союзників. |
| **Органи НАТО з координації запобігання кіберзагрозам** |
| Загальну імплементацію Політики з кібероборони НАТО здійснює **Північно-Атлантична Рада**.  Їй підпорядковується **Комітет кібероборони**, який здійснює загальне управління політикою кібероброни.  На робочому рівні **Рада управління з кібероборони** (NATO Cyber Defence Management Board, CDMB) відповідає за координацію дій у сфері кібероборони між різними інституціями НАТО та країнами-членами. |
| В НАТО також діють **Рада консультацій, контролю й управління** (NATO Consultation, Control and Command (NC3) Board) та інші органи, які відповідають за ті чи інші питання кібероборони. |
| **Операційними органами Альянсу у сфері кібербезпеки** є:  - Центр операцій у кіберпросторі (Cyberspace Operations Centre), створений рішенням Брюссельського 2018 року саміту НАТО;  - Центр можливостей з реагування на комп’ютерні інциденти (NATO Computer Incident Response Capability, NCIRC) – виконує завдання із захисту мереж НАТО та надає централізовану цілодобову підтримку комп’ютерним ресурсам Альянсу;  - Групи швидкого реагування у кіберсфері (NATO Cyber Rapid Reaction teams) - перебувають у постійній готовності надати допомогу союзникам. |
| **Центр передового досвіду із кібероборони** (NATO Cooperative Cyber Defence Centre of Excellence, CCD CoE), створений у 2008 р. й розташований в Таллінні в Естонії, який здійснює дослідження, проводить навчання і тренування у сфері кібербезпеки, а також Школа НАТО з комунікацій та інформаційних систем (NATO Communications and Information Systems School, NCISS), Школа НАТО в Обераммергау в Німеччині (NATO School in Oberammergau) та Оборонний коледж НАТО в Італії, які виконують функцію підготовки спеціалістів з кібероборони. |
| **Україна** |
| 2007 р. створена **Команда реагування на комп’ютерні надзвичайні події** України (Computer Emergency Response Team of Ukraine, CERT-UA), яка є спеціалізованим структурним підрозділом ДССЗЗІ. Вона виконує роль технічного координатора державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів  Стратегія національної безпеки України 2015 р. містить блок кіберзагроз національній безпеці держави – «Загрози кібербезпеці і безпеці інформаційних ресурсів».  Стратегією до **переліку актуальних загроз**, що здійснюються Росією «для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території», віднесено «загрози кібербезпеці і безпеці інформаційних ресурсів:  - уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;  - фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом».  Основні **напрями державної політики національної безпеки** України передбачають спеціальний розділ «Забезпечення кібербезпеки і безпеки інформаційних ресурсів» **Пріоритетами забезпечення кібербезпеки** і **безпеки інформаційних ресурсів визначено**:  - розвиток інформаційної інфраструктури держави;  - створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп’ютерні надзвичайні події (CERT);  - моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;  - розвиток спроможностей правоохоронних органів щодо розслідування кі-  берзлочинів;  - забезпечення захищеності об’єктів критичної інфраструктури, державних  інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;  - реформування системи охорони державної таємниці та іншої інформації з  обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС;  - створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;  - розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки |
| 2016 року була схвалена Стратегія кібербезпеки України  2017 року закон «Про основні засади забезпечення кібербезпеки України» |
| Закон України «Про національну безпеку» (21.06.2018 р.) в ст. 19 покладає на Службу безпеки України забезпечення кібербезпеки.  Ст. 22 Закону відзначає особливу роль Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ): «є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку,  формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації |
| **Воєнною доктриною України, схваленою 24 вересня 2015 року, питання кібероборони обійдені увагою** |
| Основу національної системи кібербезпеки складають СБУ, ДССЗЗІ, Міністерство оборони та Генеральний штаб ЗС України, Національна поліція, Національний банк України, розвідувальні органи.  **Вищим координаційним органом** є Національний координаційний центр  кібербезпеки як робочий орган **РНБО України**. Основні завдання Центру  є вироблення пропозицій з посилення спроможностей України у боротьбі із  кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом, кіберзлочинністю та у забезпеченні кіберзахисту інформаційних ресурсів і критичної інфраструктури. |
| **ЄС допомагає Україні завдяки своїй Консультативній місії** (EU Advisory Mission to Ukraine, EUAM), яка по всій Україні допомагає серед іншого у сфері протидії кіберзагрозам. На різноманітні проекти допомоги Україні у сфері кібербезпеки в КМЄС було виділено більше **2,5 млн євро**. Місія сприяє покращенню технічного оснащення українських правоохоронних органів, проводить тренінги, обміни досвідом, дискусійні панелі. До заходів залучаються фахівці Європолу та інших інституцій ЄС. |
| Кіберсфера є пріоритетною у розвитку співробітництва України з **НАТО**. Українські експерти, які взяли участь у міжнародному круглому столі «Україна-НАТО: Невійськова співпраця як спільна відповідь на гібридні загрози» |
| **Кібербезпека на другому місці серед пріоритетних напрямків спільної Україна-НАТО протидії гібридним загрозам** |
|  |
| Співпраці Україна-НАТО **сприяє** запущений у 2014 році відповідний Трастовий фонд допомоги Альянсу (Trust Fund on Cyber Defence) та Комплексний пакет допомоги НАТО, схвалений 2016 року, де кібербезпека визначена пріоритетним напрямком |
| Мета: забезпечити розвиток в Україні власних груп протидії кіберзагрозам та надійних захисних технічних можливостей CSIRT1, включаючи лабораторії для розслідування кіберінцидентів. |
| У 2014 році розпочато проект із створення **ситуаційних центрів реагування на комп’ютерні інциденти** для моніторингу подій у сфері кібербезпеки, а також лабораторій для розслідування інцидентів у кіберпросторі та ліквідації їхніх наслідків.  У 2017 року українські інституції отримали відповідне обладнання, а в липні 2017 року завершився перший етап Цільового фонду, головними бенефіціарами якого були СБУ та ДССЗЗІ.  У січні 2018 року був відкритий **Ситуаційний центр забезпечення кібербезпеки СБУ**. На цей проект НАТО виділило понад **1 млн. доларів** США. Інші українські міністерства, зокрема, МЗС України, також отримують від НАТО обладнання та програмне забезпечення, необхідне для захисту інформаційної інфраструктури |
| Україна є однією з країн-партнерів, які беруть участь у **навчальній програмі з кібербезпеки Програми НАТО** «Удосконалення військової освіти» (Defence Education Enhancement Programme, DEEP). Так, у вересні 2018 року такий курс був проведений на базі Житомирського військового інституту імені Сергія Корольова, під час якого були відпрацьовані оборонні і наступальні кібер-операції на підтримку військовій місії. |
| Щороку українські військові фахівці у сфері кібероборони беруть участь в  **масштабному багатонаціональному навчанні НАТО «CWIX”** (Coalition Warrior Interoperability Exercise), які проводяться у тренувальному центрі в Бидгощі в Польщі. |
| **Сучасні виклики та загрози кіберпростору України** |
| Група хакерів з числа низки груп постійних загроз (Advanced Persistent Threat), що проводить інформаційні операції на замовлення російського уряду (АРТ 28, Fancy Bear, Pawnstorm, CyberCaliphate, Cyber Berkut, Tsar Team та ін.), - ідентифікована як кібер-підрозділ ГУ ГШ ЗС РФ. Спеціалізація APТ 28: добування інформації з оборонної, військово-політичної та геополітичної тематики. Об’єктами атак були комп’ютерні мережі низки державних установ та організацій країн Центральної і Східної Європи, зокрема, Польщі, Чехії, України, Грузії, а також НАТО та ОБСЄ. |
| З 2014 року Україна використовується як полігон для тестування російськими спецслужбами нових практик кібератак. |
| 2012 р. МО РФ спільно з Агентством стратегічних ініціатив, Міністерством освіти і науки РФ та Московським вищим технічним училищем ім. Баумана оголосило всеросійський конкурс науково-дослідних робіт, одна з тем якого – «Методи і засоби обходу антивірусних систем, засобів мережевого захисту, засобів захисту операційних систем» |
| Указ президента РФ В. Путіна № 31с від 15 січня 2013р., - на ФСБ РФ покладена відповідальність за створення системи кіберзахисту та протидії кібератакам на російську критичну інфраструктуру. Включає підрозділ інформаційного протиборства в Генштабі ЗС РФ.  2013 р. - Створення військ інформаційних операцій.  Начальник Генштабу ЗС РФ у 2004-2008 р.р. генерал армії Юрій Балуєвський: «*Перемога над противником в цій війні може бути набагато важливіше, ніж перемога в класичному військовому протистоянні, оскільки вона безкровна, а ефект вражаючий - знекровлює і паралізує всі органи влади держави-супротивника*».  МО, ФСБ, ФСО та ФСТЭК мають однакові можливості. |
| **Український кіберфронт російської гібридної агресії** |
| 2014 р. група «КіберБеркут» (АРТ 28) взяла на себе відповідальність за атаки на сайти державних органів і громадських організацій України та низки західних країн.  Перші атаки були здійснені в березні 2014 року під час окупації Криму,  коли був тимчасово заблокований ряд українських веб-ресурсів і було оголошено про атаку на три інтернет-ресурси НАТО.  Значущі акції «КіберБеркуту» в інформаційному і кіберпросторі:  - створення перешкод у роботі ЦВК України напередодні виборів Президента України 23 травня 2014 року;  - блокування роботи сайтів МВС України та Генеральної прокуратури України 4 квітня 2014 року;  - DDoS-атаки на веб-сайт Кабінету Міністрів України 10 і 14 квітня 2014 року;  - блокування телефонів стільникового зв’язку членів уряду України;  - блокування провідних новинних порталів УНІАН і ЛІГАБізнесІнформ;  - блокування сайту президента України П. Порошенка 29 липня 2014 року. |
| 2015 р. за підтримки російських силових органів створена хакерська організація під назвою «СПРУТ» («Система протидії українському тероризму»). Дана організація проводить атаки на офіційні сайти керівництва обласних державних адміністрацій, Міністерства оборони України, Служби безпеки України, Генерального штабу ЗС України,  Головного управління розвідки МО України. |
| 2015 року для підвищення ефективності інформаційної війни проти України керівництво Генштабу ЗС Російської Федерації створило в складі  Центру територіальних військ Південного військового округу РФ **Центр інформаційного протиборства (ЦІП) в Новочеркаську**. В Донецьк було доставлено потужний програмно-апаратний комплекс, призначений для проведення розподілених кібератак (DDoS-атаки). |
| У 2013-2017 роках **кібератаки проти України** здійснювалися з використан  ням АРТ-атак (Snake, Uroboros, Sofacy/APT28, Epic Turla, Black Energy 2 і  3, Armageddon та інші), характерних саме для України.  У червні 2017 року Україна зазнала масштабної атаки комп’ютерного вірусу Petya-A, що проник до низки мереж українських державних і приватних установ, зокрема, сайту Кабміну і ряду міністерств, Пенсійного фонду, КМДА, низки банків, крупних державних і приватних підприємств. Кіберполіції України вдалося зупинити наступну хвилю кібератаки та встановити, що їй передував збір даних про підприємства України. |
| **В Росії напрацьовані зразки кіберзброї для нейтралізації критичної інфраструктури противника з метою підвищення ефективності послідуючого першого удару** або ж максимального послаблення його спроможностей чинити опір. Характерним є те, що дія такого роду кіберзброї прирівнюється до обеззброюючого ядерного удару.  (подібна кіберзброя не може мати ніякого потенціалу стримування). |

ВИСНОВКИ

Зростаючий масив компютерних технологій сприяє транснаціональному розширенню масштабу комп’ютерних мереж. Це збільшує їх вразливість та створює можливості для їх неправильного використання, в т.ч. на транснаціональній основі.

Встановлено, що останніми роками відбувається зростання кіберзлочинів, серед яких і злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Значення автоматизованих систем управління, комунікації, САУП, комп’ютерних мереж та мереж електрозв’язку, включно, мобільного зв’язку наразі є невідємною частиною сучасного суспільства, економіки, управління, безпеки.

У цифрову епоху, коли спілкування в Інтернеті стало нормою, користувачі Інтернету, уряди та бізнес стикаються з підвищеними ризиками стати об’єктами кібератак.

Загрози можуть мати різне походження, включаючи кримінальні, політично вмотивовані, терористичні або фінансовані державою напади, а також стихійні лиха та ненавмисні помилки. За останні кілька років світовий ландшафт кіберзлочинності кардинально змінився, і злочинці, які використовують більш досконалі технології та більше знань про кібербезпеку.

Запобігання злочинам у сфері цифрових (комп’ютерних) технологій наразі грунтується на комплексному підходів виконання завдань у сферах: правовій, організаційній, матеріально-технічній, правоохоронній.

В Україні вживаються заходи в напрямку комплексного вирішення завдань. Так, в КК України закріплено окремі склади злочинів в межах одного спеціалізованого Розділу щодо злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Об’єктивно, що КК України містить матеріальні норми, які складають санкцію за злочин, вчинений у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Запобігання цим злочинам на основі одного лише КК України малоефективне, оскільки більшість злочинців в цій сфері покладаються на анонімність мережі Інтернет, де навіть у випадку визначення статичної чи динамічної IP адреси, притягнення злочинця до відповідальності вкрай проблематичне, оскільки відсутня персоніфікація суб’єкта.

В умовах відсутності кордонів скоєння кіберзлочинів запорукою стратегічного запобігання кіберзлочинів є узгоджене міжнародне співробітництво. Таким є низка заходів, створених в Європі, зокрема, на основі Конвенції про запобігання кіберзлочинам, та заходів, які здійснюються в рамках альянсу НАТО.

В рамках співробітництва необхідне: 1) узгодження матеріального права (єдності підходів в визначенні дій, які складають кіберзлочин; визначення видів злочинних дій); 2) узгодження процесуального права (юрисдикції, екстрадиції, вжиття запобіжних заходів, термінового збереження комп'ютерних даних, які зберігаються; термінового збереження і часткового розкриття даних про рух інформації; обшук і арешт комп'ютерних даних, які зберігаються; збирання даних про рух інформації у реальному масштабі часу; перехоплення даних змісту інформації); 3) узгодження спільних дій; 4) узгодження спільної допомоги; 5) обмін інформацією.

Тому для вирішення в Україні питання запобігання злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, варто забезпечити імплементацію міжнародних стандартів протидії, запобігання та боротьби з цими злочинами:

* єдині підходи до розуміння компютерного злочина та його видів;
* гармонізація кримінального законодавства сприяє створенню міжнародних норм поведінки для використання комп’ютера встановлює позитивні норми поведінки та служить вихованню та стримуванню;
* гармонізація може допомогти уникнути ринкових обмежень та національних бар'єрів для вільного потоку інформації та передачі технологій;
* гармонізація законів, включаючи кримінальне, може сприяти рівним умовам конкуренції. Неналежний правовий захист комп’ютерних програм, технологій або комерційної таємниці в деяких країнах може призвести до того, що деякі компанії працюватимуть там таким чином, який інші країни вважатимуть недобросовісною конкуренцією;
* гармонізація може перешкодити деяким країнам перетворитися на притулки, з яких міжнародні комп’ютерні злочини можуть вчинятися безкарно;
* гармонізація полегшує правоохоронну діяльність органами різних країн, оскільки вона забезпечує загальне розуміння того, які типи поведінки становлять злочин, і, зокрема, злочинність, пов’язану з комп’ютером;
* гармонізація сприяє вирішенню питань екстрадації;
* гармонізація полегшує взаємну правову допомогу, використання підконтрольних закону слідчих повноважень: пошуку та вилучення, допиту свідків, електронного спостереження тощо, однією країною на користь іншої країни;
* гармонізація правопорушень сприяє гармонізації процесуального законодавства щодо повноважень слідства.

Основними проблемами в сфері запобігання кіберзлочинам в Україні наразі є: 1) низький рівень фахової підготовки спеціалістів; 2) нестача фахівців, низький рівень мотивації співробітників правоохоронних органів; 3) майже принципове небажання слідчих, експертів та оперативних працівників користування методичними посібниками та стандартами; 4) низький рівень взаємодії та партнерства правоохоронних органів та приватного сектору у сфері кіберзахисту; 5) обмеження кіберзлочинів в КК України лише злочинами у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку; 6) неналежний рівень імплементації положень Конвенції Ради Європи «Про запобігання кіберзлочинів» в КПК України щодо: вжиття запобіжних заходів, блокування «ризикового тарфіку та ризикових операцій», проведення окремих видів слідчих дій; 7) протиріччя КПК України та Закону України «Про оперативно-розшукову діяльність» (у Законі України «Про ОРД» наводяться два поняття, які містять суперечнос­ті, створюючи колізію правових норм: обов’язок оперативно го підрозділу здійснювати профілактику правопорушень (п. 1 ч. 1 ст. 7 Зако­ну) та: користуватися своїми правами лише для вико­нання завдань оперативно-розшукової діяльності (ч. 1 ст. 8 Закону), у змісті яких немає профілактики, попередження, запобігання); 8) невідповідність норм КПК України щодо накладання арешту відповідно до Постанови слідчого судді потребам терміновості блокування сумнівних цифрових (і в першу чергу, банківських операцій).

Визначено, що для потреб ОРД є потреба в: 1) нормативній регламентації оперативно-розшукових дій стосовно кіберсередовища; 2) розробці актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі; 3) удосконаленні системи інформаційно-аналітичного забезпечення; 4) гармонізації кримінального законодавства про кіберзлочини; 5) імплементації міжнародних процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з ура­хуванням транскордонної проблеми; 6) налагодженні співробітництва право­охоронних органів при розслідуванні кіберзлочинів на оперативному рівні; 7) створенні швидких та дієвих механізмів вирішення юрисдикційних питань у кіберпросторі; 8) зобов’язанні компаній збері­гання резервних копій електронних даних; 9) полегшенні доступу правоохоронних органів до електронних банків даних; 10) удосконаленні стандартів забезпечення заходів безпеки на об’єктах критичної інфрастуруктури. На рівні Держспецзв’язку України доцільно ввести стандарти та методичні рекомендації для основних галузей об’єктів критичної інформаційної інфраструктури та державних органів. Ці рекомендації мають розроблятися з урахуванням міжнародних практик та стандартів розвитку груп реагування на інциденти, що пов’язані з кібербезпекою (CERT та CSIRT/SOC).

Впровадження міжнародних стандартів має враховувати досід функціонування організації, подібної до NIST, яка мог­ла б формалізувати систему управління ризиками для державних органів та приватних суб’єктів, долучити їх до відкритої дискусії про загрози, вразливості, стійкість до ризиків, а також можливість їх зниження в кіберкомпонентах сфери національної безпеки України. За допомогою такої організації можна організовувати і впроваджувати програми навчання і підвищення кваліфікації, стажування та обміну між компаніями, що займаються кібербезпекою, і державними органа­ми, а також налагодити співпрацю та обмін співробітниками між групою швидкого реагування (CERT-UA) та іншими групами швидкого реагування об’єктів критичної інформаційної інфраструктури.

Загрози з боку іноземних держав, та в першу чергу, РФ, в т.ч. у сфері кібербезпеки на рівні національної безпеки, потребує подальшу співпрацю з структурами безпеки (безпеки оборони) ЄС та Альянсу НАТО, які мають організаційну структуру, матеріально-технічне забезпечення, програмне забезпечення, та забезпечують обмін інформацією, спільні практичні навчання та взаємодію в напрямку забезпечення національної безпеки на рівні кібербезпеки.

Об’єктивно, що притягнення до кримінальної відповідальності є необхідністю для пропаганди належної поведінки у кіберпросторі та запобіганню злочинів в цій сфері. Наразі заслуговує на увагу Вирок Комунарського районного суду м. Запоріжжя від 10.03.2020 р. у справі № 333/714/20, за якою обвинувачений, використовуючи комп'ютерну техніку, здійснив несанкціоноване втручання до особистого кабінету потерпілого й отримав доступ до його облікового запису в онлайн-грі «World of Tanks», після чого продав його невстановленій особі через Інтернет.

Однак, з погляду на пріоритет «безпеки», який вже є прямо залежним від належного функціонування комп’ютерних систем та мереж і мереж електрозв’язку, пріоритетна увага має приділятися фізичному (на технологічному та операційному рівнях) запобіганню кіберпідрозділами як правоохоронних органів, так і розвідки та контррозвідки, СБУ та, мабуть, особливо, Міністерства оборони України, для чого їм мають бути надані широкі повноваження негайного реагування (в першу чергу, блокування кібератак) та збору «електронних доказів», їх копіювання та дослідження, правової регламентації обшуків та виїмок «цифрових данних».

В сфері взаємодії НАТО варто: 1) довести до робочого рівня систему координації у сфері кібербезпеки відповідно до Стратегії кібербезпеки України; 2) використати досвід та практики ЄС і НАТО для створення широкої національної схеми сертифікації з кібербезпеки, розробки плану відповіді відповідати на широкомасштабні інциденти і кризи; 3) посилити державно-приватне партнерство; 4) приєднатися до Центру передового досвіду НАТО з кібероборони для поглиблення співпраці України з Альянсом; 5) розвинути співробітництво з посилення кібербезпеки в Україні для попередження і нейтралізації можливого російського втручання в Україні; 6) продовжити визначення критичної інфраструктури та її ключових операційних вразливостей; 7) розробити План реагування на надзвичайні ситуації в кіберпросторі; 8) створити хмарні сервіси для збереження інформації.

ПЕРЕЛІК використаних джерел

1. Алєксєєва-Процюк Д.О. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Випуск 2. С. 247-253.
2. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414-418.
3. Бенджамин С., Бакленд. Демократическое управление и вызовы кибербезопасности. Женева: Женевский центр демократического контроля над вооруженными силами. 2013. 47 с.
4. Бугера О.І. Загальна кримінологічна характеристика мережі інтернет та запобігання злочинності. *Право і суспільство. 2018. № 5. С. 177-181.*
5. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності. *Актуальні питання розслідування кіберзлочинів*: матеріали Міжнародної науково-практичної конференції (Харків, 10 грудня 2013 р.). Харків: Харківський національний університет внутрішніх справ, 2013. С. 179-182.
6. Бутузов В. М. Співвідношення понять «комп’ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави*. 2010. № 1 (3). С. 18.
7. Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика*). 2018. Вип. 1-2 (10-11). С. 276-282.
8. Воєнна доктрина України: затверджена Указом Президента України від 24 верес. 2015 р. № 555/2015. *Офіційний вісник України*. 2015. № 78.
9. Гетьман Г.М. Сліди злочинів у сфері використання електроннообчислювальних засобів, телекомунікаційних систем і комп’ютерних мереж. *Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції* : монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Вид. агенція «Апостіль», 2017. 260 с. С. 52-62.
10. Голіна В., Головкін Б. Кримінологія: Загальна та Особлива частини: навчальний посібник. Xарків: Право, 2014. 513 с.
11. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1(28). С. 118-128.
12. Демедюк С.В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні. *Південноукраїнський правничий часопис*. 2015. № 3. С. 119-123.
13. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 6-17.
14. Додатковий протокол до Конвенції про кіберзлочинність. який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи від 28.01.2003 р. Протокол ратифіковано із застереженням Законом № 23-V від 21.07. 2006 р. *Відомості Верховної Ради України*. 2006. № 39. Ст. 328.
15. Доктрина інформаційної безпеки України: Затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення 04.09.2020 р.)
16. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право*. 2017. № 1. С. 104-111.
17. Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. *Теорія і практика правознавства*. 2013. Вип. № 2. С. 1-11.
18. Задерейко О.В., Лигинова Н.І., Троянський О.В. Сучасне кіберсередовище держави як театр бойових дій : *Кібербезпека в Україні: правові та організаційні питання* : матеріали всеукр. наук. - практ. конф., м. Одеса, 17 листопада 2017 р.». Одеса : ОДУВС, 2017. 204 с.
19. *Злочинність у глобалізованому світі* : матеріали XVІ Всеукр. кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. Харків : Право, 2017. 420 с.
20. Керівні принципи політики Ради Європи щодо комплексних національних стратегій із захисту дітей від насильства. URL: https://rm.coe.int/168046eb82 (дата звернення 04.09.2020 р.)
21. Кирбят’єв О.О. Комп’ютерні злочини: реалії сучасності, проблеми боротьби з ними та ймовірні шляхи їх вирішення. *Вісник Запорізького національного університету*. 2010. № 1. С. 165-170.
22. Кібербезпека в Україні – шляхи вирішення. URL: http://www.soldis-.com.ua/uk/node/699 (дата звернення 04.09.2020 р.)
23. Кількість кіберзлочинів в Україні зросла вдвічі за останні п’ять років - Opendatabot. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukray-ini-zrosla-vdvichi-za-ostanni-p-yat-rokivopendatabot (дата звернення 04.09.2020 р.).
24. Коваленко Н.В. Про правовий режим кібербезпеки в Україні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. Вип. 3. С. 96-100.
25. Конвенція про кіберзлочинність від 23.11.2001 р. *Відомості Верховної Ради України*. 2006. № № 5-6. Ст.71.
26. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
27. Костенко О.В. Сучасна правова модель суспільних відносин сфери електронних довірчих послуг в Україні. *International Journal of Innovative Technologies in Social Science*. 2019. 2(14), February. С. 3-7.
28. Кравцова М. А. Понятие киберпреступности и ее признаки. *Часопис Київського університету права*. 2015. № 2. С. 320–324.
29. Кримінальний кодекс України від 05.04.2001 р. *Відомості Верховної Ради України (ВВР)*. 2001. № 25-26. Ст. 131.
30. Кримінальний процесуальний кодекс України: Науково-практичний коментар / Відп. ред.: С. В. Ківалов, С. М. Міщенко, В. Ю. Захарченко. Х.: Одіссей, 2013. 1104 с.
31. Кримінологія: підручник для студентів вищих навч. закладів / О. Джужа, Я. Кон­дратьев, О. Кулик, П. Михайленко та ін.; за заг. ред. О. Джужи. К.: Юрінком-Інтер, 2002. 416 с.
32. Лук’янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник НАДУ*. 2015. №4. С. 50-56.
33. Манжай О.В. Окремі правила роботи працівників ОВС у комп’ютерних соціальних мережах. *Використання інноваційних технологій у попередженні злочинів* : матеріали наук.-практ. семінару (м. Харків, 6 груд. 2012 р.). МВС України, Харк. нац. ун-т внутр. справ. Харків : ХНУВС, 2012. С.100-102.
34. Марков В. В. Хакерські атаки на імплантати як один із способів протиправного використання кіберпростору: сутність та види. *Вісник Харківського університету внутрішніх справ*. 2014. № 2. С. 139-147.
35. Міністр інфраструктури прокоментував наслідки кібератаки, 25.10.2017 р. URL: https://www.ukrinform.ua/rubric-technology/2331042-ministr-infrastru-kturi-prokomentuvav-naslidki-kiberataki.html (дата звернення 04.09.2020 р.)
36. Музика А.А. Законодавство України про кримінальну відповідальність за «комп’ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. Київ: Вид. ПАЛИВОДА А. В., 2005. 120 с.
37. Петровський О.М., Лівчук С.Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Young Scientist*. 2019. № 12.1 . С. 55-59.
38. Пивоваров В. В. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3, ч. 2. С. 177–182.
39. Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон : Наказ Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 03.04.2008 р. № 284/287/214/150/64/175/266/75. *Офіційний вісник України*. 2008. Ст. 1249.
40. Положення про Національний координаційний центр кібербезпеки: Указ Пре­зидента України від 7 червня 2016 р. № 242/2016. URL: http://zakon-.rada.gov.ua/laws/ show/242/2016 (дата звернення: 16.09.2020 р.)
41. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України : Наказ Адміністрації Державної прикордонної служби України від 30.09.2008 р. № 810. URL: https://zakon.rada.gov.ua/laws/show/z1086-08 (дата звернення 04.09.2020 р.)
42. Про затвердження Порядку взаємодії інформаційних систем Державної фіскальної служби України та Державної прикордонної служби України щодо обміну інформацією, необхідною для забезпечення контролю при переміщенні осіб та транспортних засобів через державний (митний) кордон України та адміністративний кордон вільної економічної зони «Крим» : Наказ Державної фіскальної служби України, Міністерства внутрішніх справ України від 07.09.2017 р. № 746/759. *Офіційний вісник України*. 2017. № 85. ст. 2585.
43. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. *Відомості Верховної Ради України (ВВР).* 1994. № 31. Ст. 286.
44. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського парламенту і Ради (ЄС) від 6 липня 2016 року № 2016/1148. URL: https://zakon-.rada.gov.ua/laws/show/984\_013-16/sp:max100?sp=:max&lang=uk (дата зверне-ння 04.09.2020 р.)
45. Про інформацію: Закон України від 02.10.1992 р. *Відомості Верховної Ради України (ВВР).* 1992. № 48. Ст. 650.
46. Про Концепцію розвитку сектору безпеки і оборони України: Указ Президента України № 92/2016 від 04.03. 2016 р. URL: https://zakon.rada-.gov.ua/laws/show/n0002525-16 (дата звернення 04.09.2020 р.)
47. Про невідкладні заходи щодо забезпечення інформаційної безпеки України: Рішення Ради національної безпеки і оборони України: введеному в дію Указом Президента України від 23 квітня 2008 року № 377/2008. (Скасовано Рішенням Ради національної безпеки і оборони України від 28.04.2014 р.). URL: https://zakon.rada.gov.ua/laws/show/n0008525-14 (дата звернення 04.09.2020 р.)
48. Про основи національної безпеки: Закон України від 21.06.2018. *Відомості Верховної Ради (ВВР)*. 2018. № 31. Ст. 241.
49. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
50. Про особливе партнерство між Україною та ОрганізацієюПівнічно-Атлантичного договору : Хартія від 9 лип. 1997 р. № 994. URL: https://zakon-.rada.gov.ua/laws/show/994\_002#Text (дата звернення 04.09.2020 р.)
51. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 23.11.2001 р. *Відомості Верховної Ради України*. 2006. № 5-6. Ст. 71.
52. Про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. № 287/2015. *Офіційний вісник України*. 2015. № 43. Ст.1353.
53. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» : Указ Президента України від 14.03.2016 р. № 92/2016. URL: https://zakon-.rada.gov.ua/laws/ show/92/2016 (дата звернення 04.09.2020 р.)
54. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : Розпорядження Кабінету Міністрів України від 24.07.2019 р. № 687-р. *Урядовий кур’єр*. 2019. № 170.
55. Пфо О.М. Основні поняття і класифікація кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки*: матеріали Всеукраїнської науково-практичної конференції (23-25.11.2016 р. Кропивницький. С. 33-34. URL: https://core.ac.uk/download/pdf/84825482.pdf (дата звернення 04.09.2020 р.).
56. Раєцький А. Кібербезпека бізнесу це не лише технічні заходи. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/ (дата звернення 07.09.2020 р.)
57. Ращенко Є. Кримінально-правове забезпечення боротьби зі злочинами у сфері використання комп’ютерних технологій. *Право України*. 2013. № 10. С. 87-91.
58. Русецькнй А., Куцолабський Д., Теоретнко-правовнй аналіз понять «кіберзлочнн» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74-78.
59. СБУ встановила причетність спецслужб РФ до атаки вірусу Petya-A, 01.07.2017. URL: https://www.ukrinform.ua/rubric-technology/2257453-sbu-vsta-novila-pricetnist-specsluzb-rf-do-ataki-virusupetyaa.html (дата звернення 04.09.2020 р.)
60. СБУ попереджає про можливу кібератаку на установи та підприємства, 18.08.2017 р. URL: https://www. ukrinform.ua/rubric-society/2288607-sbu-poperedzae-pro-mozlivu-kiberataku-na-merezi-ukrainskihustanov-ta-pidpriemstv-.html (дата звернення 03.09.2020 р.)
61. Семенов В., Дзігора М. До питання боротьби з кіберзлочинністю в Україні. *Прикарпатський юридичний вісник*. Випуск 6 (15). 2016. С. 174-178.
62. Сіренко О.В. Поняття кіберзлочинів та особливості методики їх розслідування. *Кібербезпека в Україні: правові та організаційні питання*: матеріали всеукр. наук.-практ.конф., м. Одеса. ОДУВС, 2017. С.48-49.
63. Солдатова В. Окремі заходи попередження і боротьби з кіберзлочинністю. *Віс­ник Кримінологічної асоціації України*. 2013. № 3. С. 145-155.
64. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Центр глобалістики «Стратегія ХХІ». URL: http://geostrategy.org.ua (дата звернення 09.09.2020 р.)
65. Столяр О. Міжнародно-правові проблеми визначення та класифікації «кіберзлочинів». *Jurnalul juridic national: teorie si practica*. Ijulie 2017. С. 190-193
66. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: https://www.president.gov.ua documents/962016-19836 (дата звер­нення: 16.08.2020 р.).
67. Ступник Я., Когут М. Протидія наркозлочинності в мережі Інтернет: виклики сього­дення. *Науковий вісник Ужгородського національного університету. Серія «Право».* Випуск 26. 2014. С. 226-230.
68. Тавожанський О.В. Кримінологічні аспекти кіберзлочинності у сучасних умовах. *Журнал східноєвропейського права*. 2016. №. 31. С. 80-86.
69. У СБУ відбулася церемонія завершення першого етапу Трастового фонду НАТО зі сприяння Україні в зміцненні кіберзахисту. 04.07.2017. URL: https://www.ssu.gov.ua/ua/news/1/category/2/view/3668#.V3SsDFLC.dpbs (дата звернення 04.09.2020 р.)
70. Фурман В. Кіберзлочинність. Проблеми доказування. *Аналітичне видання “Юрист&Закон”. Випуск №45.* URL: https://artius.ua/novini/statti/ kiberzlochinnist-problemi-dokazuvannya.html (дата звернення 03.09.2020 р.)
71. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони*. №4 (58). 2017. С.80–85.
72. Эрман Г. Готовьтесь, потому что Россия нанесет киберудар по Украине - эксперт из США. BBC News Украина. 04.06.2018 р. URL: https://www.bbc-.com/ukrainian/features-russian-44353054 (дата звернення 04.09.2020 р.)
73. Яцик Т.П. Розслідування інформаційного тероризму та кіберзлочинності (міжнародно-правовий аспект).  *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2017. Вип. 1 (5). С. 111-115.
74. Baron L . (2006). Gone Vishing. *Journal of Accountancy*. 2006. 202(3). Pp. 15.
75. Bergholz A., De beer J., Glahn s., Moens M.-F., Paass G. Strobel S. (2010). New filtering approaches for pshishing email. Journal of computer security. 2010. № 1. P.p.7-35.
76. Bishop J. (2013). The effect of deindividuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater. *International Journal of Cyber Criminology*. 2013. № 7(1), pp. 28-48.
77. Bose I., Leung A. C. M. (2007). Unveiling the mask of phishing: threats, preventive, measures and responsibilities. *Communications of the Association of InformationSystems.* 2007. № 19. Р.р. 544-566.
78. Carter D.L. Computer Crime Categories: How Techno-Criminals Operate. *FBI Law Enforcement Bulletin*. 1995. Volume: 64, Issue 7. рp. 21-27.
79. Castells M. (2002). The internet galaxy: Reflections on the internet, business and society, Oxford: Oxford University Press. URL: https://www.researchgate-.net/publication/249471554\_The\_Internet\_Galaxy\_Reflections\_on\_the\_Internet\_Business\_and\_Society\_By\_Manuel\_Castells (дата звернення 04.09.2020 р.).
80. Clough J. (2010). Principles of cybercrime. Cambridge University Press. URL: https://www.cambridge.org/core/books/principles-of-cybercrime/ (дата звернення 11.09.2020 р.).
81. Cybercrime. URL: https://www.interpol.int/Crimeareas/Cybercrime (дата звернення 04.09.2020 р.).
82. European Commission (2013). Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: COM (2013) 01 final, 07 February 2013. URL: http://eur-lex.europa.eu/legalcontent/EN/ALL/?uri= (дата звернення 04.09.2020 р.).
83. European Commission (2015). Special Eurobarometer cybersecurity report, February 2015. URL: http://ec.europa.eu/public\_opinion/archives/ebs\_423\_en.pdf (дата звернення 04.09.2020 р.).
84. European Crime Prevention Network Theoretical Paper. Cybercrime. Cybercrime: A theoretical overview of the growing digital threat In the framework of the project ‘The development of the observatory function of the European Centre of Expertise on Crime Prevention within the EUCPN’ - EUCPN Secretariat, February 2016, Brussels. URL: https://eucpn.org/sites/default/files/document/ theoretical\_paper\_cybercrime\_.pdf (дата звернення 04.09.2020 р.).
85. Europol (2014). The Internet Organised Threat Assessment (iOCTA) 2014. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-or-ganisedcrime-threat-assessment-iocta-2014\_paper\_cybercrime\_.pdf (дата зверне-ння 04.09.2020 р.)
86. Gercke M. Understanding cybercrime: a guide for developing countries. *International Telecommunication Union (Draft)*. 2011. Vol. 89, p. 93.
87. Gordon S., Richard, F. (2006). On the definition and classification of Cybercrime. *Journal in Computer Virology.* 2006. Volume 2. Issue 1. pp. 13-20.
88. Gosh S., Turrini E. (2011). Cybercrimes: A Multidisciplinary Analysis, Springer. URL: https://eucpn.org/sites/default/files/document/files/theoretical (дата звернення 04.09.2020 р.).
89. Grabosky P.N. (2001). Virtual criminality: Old wine in new bottles?. *Social and Legal Studies* URL: http://journals.sagepub.com/doi/10.1177/a017405 (дата звернення 11.09.2020 р.)
90. Halder D., Jaishankar K. (2011). Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. *Hershey, PA, USA.* URL: https://www.igi-global.com/book/cyber-crime-victimization-women/50518 (дата звернення 14.09.2020 р.).
91. Iatsyk T.P. Media terrorism and cyberterrorism as problem of information society (criminal procedure aspect). *Міжнародний юридичний вісник: збірник наукових праць Національного університету державної податкової служби України*. 2016. Вип. 2(4). С. 139–143.
92. ISO/IEC 27552 - Information technology - Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management - Requirements and guidelines [DRAFT]. URL: https://www.iso27001-security.com/html/27552.html (дата звернення 04.09.2020 р.).
93. Luppicini R. Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media J. (Canadian Edition).* 2014. Vol. 7 (№ 1). P. 35-50.
94. Mittal S. Perspectives in Cyber Security, the future of cyber malware. *The Indian Journal of Criminology*. Vol. 41, p. 18.
95. Mittal S. The Issues in Cyber- Defense and Cyber Forensics of the SCADA Systems. *Indian Police Journal.* Vol. 62, pp. 29- 41.
96. Moore R. (2015). Cybercrime: investigating high-technology computer crime. *Routledge*. p. 4. URL: http://www.worldcat.org/title/cybercrime-investigating-high-technology-computer-crime/oclc/893676642 (дата звернення 04.09.2020 р.)
97. Net Losses Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies. 2014. URL: http://www.mcafee.com/us/resources-/reports/rp-economicimpact-cybercrime2.pdf (дата звернення 04.09.2020 р.).
98. Proteus Manual (2015). Prevention, Information and support to victims of online identity theft. 2015, Lisboa, APAV. URL: https://www.apav.pt-/proteus/images-/Proteus\_PDF/ManualDeProcedimentosProteus-UK.pdf (дата звернення 03.09.2020 р.).
99. Schoofs P. (2014). Phishing bij de overheid in België. Masterproef Business Process Management and IT; Open Universiteit Heerlen. URL: https://eucpn.org-/sites/default/files/document/files/theoretical\_paper\_cybercrime\_.pdf (дата зверне-ння 04.09.2020 р.). (дата звернення 04.09.2020 р.).
100. Speer D.L. Redefining borders: The challenges of cybercrime. *Crime, law and social change.* Vol. 34, pp. 259- 273.
101. Stein Schjolberg, Solange Ghernaouti-Hélie. A Global Protocol on Cybersecurity and Cybercrime. Cybercrimedata. An initiative for peace and security in cyberspace. URL: https://www.cybercrimelaw.net/documents/A\_Global\_Proto-col\_on\_Cybersecurity\_and\_Cybercrime.pdf (дата звернення 04.09.2020 р.)
102. Tyler Elliot Bettilyon. Cybersecurity Is About Much More Than Hackinghttps. URL: https://medium.com/s/story/cybersecurity-isnt-just-about-hacks-f11c7ad0766 (дата звернення 01.09.2020 р.).
103. United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime, Vienna, February 2013. URL: https://www.unodc.org/documents-/organizedcrime/UNODC\_CCPCJ\_EG.4\_2013/CYBERCRIME\_STUDY\_210213.pdf (дата звернення 04.09.2020 р.)
104. Vishwanath A., Herath T., Chen R., Wang J. G. & Roa, H. R. (2011). Why do people get phished? Testing individual differences in pshishing vulnerability within an integrated, informative processing model. *Decision Support Systems*. 2011. № 51(3). Р.р. 576-586.
105. Wall D.S. (2008). Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology*. 2008. Vol. 22, nos. 1-2, pp. 45–63.
106. Warren G. Kruse Jay, Heiser G. (2001). Computer Forensics: Incident Response Essentials. Boston, MA: Addison-Wesley. URL: https://www.help-netsecurity-.com/2002/08/18/computer-forensics-incident-response-essentials/ (дата звернення 04.09.2020 р.).
107. Workman M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology,* Volume 59, Issue 4, p.р.662–674.
108. Yar M. (2005). The Novelty of «Cybercrime»: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology.* 2005. № 2. р. 407.
109. Yar M. (2005). The Novelty of «Cybercrime»: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*. 2005. № 2. URL: https://journals.sagepub.com/doi/10.1177/147737080556056
110. Yar M. (2006). Cybercrime and society. Sage Publications Inc., London, p. 9. URL: http://sk.sagepub.com/9781446212196?seq=n3 (дата звернення 04.09.2020 р.)