**Київський національний торговельно-економічний університет**

Кафедра загальноправових дисциплін

**ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА**

на тему:

# ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ ЯК СПОЖИВАЧА ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

студентки 2 курсу 8-м групи
спеціальності 081 «Право»
спеціалізації
«Правове забезпечення безпеки
підприємницької діяльності» _____ Матвієнко Руслани Сергіївни

Науковий керівник
кандидат юридичних наук,
професор кафедри
загальноправових дисциплін _____ Шестопалова Людмила Миколаївна

Гарант освітньої програми
професор, кандидат юридичних наук,
завідувач кафедри
загальноправових дисциплін _____ Крегул Юрій Іванович

**Київ 2019**

**ЗМІСТ**

ВСТУП 3
РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА ЗАГАЛЬНОПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ ЯК СПОЖИВАЧА ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ 6
1.1. Сутність та основні підходи до визначення поняття «інформаційна безпека» в національному законодавстві і наукових дослідженнях 6
1.2. Загальноправова характеристика регулювання забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні 14
1.3. Зарубіжній досвід правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг 21
РОЗДІЛ 2 УДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ НАДАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ В УКРАЇНІ 29
2.1. Стан забезпечення інформаційної безпеки людини в Україні як споживача телекомунікаційних послуг 29
2.2. Напрями вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг 41
ВИСНОВКИ 50
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 53
ДОДАТКИ 70

# ВСТУП

*Актуальність теми дослідження.* Суттєві суспільно-політичні зміни у світі наприкінці минулого століття підштовхнули політиків і вчених звернути особливу увагу на питання безпеки. Абсолютна інформатизація життя стала причиною перетворення інформації на важливий фактор, присутність якого спостерігається майже у кожній сфері життєдіяльності суспільства. За такої ситуації інформаційна безпека стає однією з провідних та невід'ємних складових національної безпеки. Тому значна кількість вчених розглядає безпеку як складне явище, що охоплює всі сфери життєдіяльності сучасного людства. Це обумовлює необхідність більш детального вивчення правових засад її регулювання з урахуванням значення в контексті національної безпеки, що націлена на захист життєво важливих інтересів людини, суспільства і держави. Національна безпека є необхідною умовою, що забезпечує сталий розвиток суспільства, а також своєчасну нейтралізацію, виявлення та запобігання потенційним або реальним загрозам національним інтересам.

Відповідно до Конституції України безпека людини проголошена найвищою соціальною цінністю, що визначає спрямованість і зміст діяльності держави. У сучасних умовах переходу української спільноти до нового етапу свого розвитку – інформаційного суспільства – пріоритетне значення набувають питання, пов'язані із забезпеченням інформаційної безпеки людини у телекомунікацій сфері. Актуальність цього питання обумовлена тим, що споживання телекомунікаційних послуг не лише заміщує життєву необхідність безпосереднього спілкування між людьми, а й поступово перетворюється на домінуючий у національних та світових масштабах різновид соціальної взаємодії. Одночасно з тим телекомунікаційні технології та послуги, за допомогою котрих вони реалізуються, надають не тільки доступ до інформації, але виступають у ролі посередника в процесі споживання та надання інформаційних послуг. З іншого боку, комунікаційні мережі відкривають більше можливостей для злочинних дій. У зв'язку з цим можна впевнено стверджувати, що нині інформаційне піднесення будь-якої нації засноване на

телекомунікаційному підґрунті та одночасно є причиною неоднозначних для існування держави, суспільства та людини наслідків.

Перелічені вище фактори обумовлюють звернення багатьох зарубіжних та українських вчених до дослідження різних аспектів інформаційних відносин у суспільстві, забезпечення інформаційної безпеки, у тому числі й у сфері телекомунікацій. Серед них слід відмітити дослідження таких науковців, як: І.В. Арістова, О.П. Баранов, І.Р. Бондар, В.П. Горбулін, А.Б. Качинський, В.І. Гурковський, О.О. Золотар, Р.А. Калюжний, А.І. Марущак, Д.В. Сулацький та ін.

*Мета дослідження* – на підставі результатів комплексного вивчення теоретичних і загальноправових підходів до інформаційної безпеки розробити основні напрями вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг.

Відповідно до визначеної мети в роботі поставлені й вирішувались такі *завдання*:

- розкрити сутність та основні підходи до визначення поняття «інформаційна безпека» в національному законодавстві і наукових дослідженнях;
- надати загальноправову характеристику регулювання забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні;
- описати зарубіжній досвід правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг;
- проаналізувати сучасний стан забезпечення інформаційної безпеки людини в Україні як споживача телекомунікаційних послуг;
- запропонувати основні напрями вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг.

*Об'єктом дослідження* є суспільні відносини, що виникають у процесі забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні.

*Предметом дослідження* є правові засади забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні.

*Теоретичною та методологічною основою дослідження* є фундаментальні праці вітчизняних і зарубіжних вчених і практиків із питань забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг.

У процесі дослідження використовувалися як загальні методи наукового пізнання, так і спеціальні методи юридичної науки:

- діалектичний метод (дав можливість розглянути досліджуваний предмет, з'ясувати його сутність, особливості, встановити взаємозв'язки з іншими проблемами, явищами; його ми використовували в підрозділах 1.1, 1.2 та 1.3 роботи);
- логіко-юридичний метод і метод контент-аналізу – використаний для опрацювання й оцінки зарубіжних та вітчизняних наукових концепцій, національних і міжнародних нормативно-правових актів, аналітичних матеріалів із питань інформаційної безпеки – підрозділи 1.2, 1.3 та 2.2;
- статистичний метод – використаний для збирання й узагальнення емпіричних матеріалів дослідження, зокрема в підрозділі 2.1.

*Інформаційну основу дослідження* складають бази нормативних документів, вітчизняні й закордонні видання, збірники наукових праць та ін.

*Випускна кваліфікаційна робота складається* із наступних частин: вступу, двох розділів, які включають п'ять підрозділів, висновків, списку використаних інформаційних джерел та додатків.

Загальний обсяг роботи становить 73 сторінки комп'ютерного тексту. У тексті роботи розміщено 1 таблиця; 8 рисунків; список використаних інформаційних джерел містить 118 найменувань.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ТА ЗАГАЛЬНОПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ ЯК СПОЖИВАЧА ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

## 1.1. Сутність та основні підходи до визначення поняття «інформаційна безпека» в національному законодавстві і наукових дослідженнях

На побутовому рівні під інформаційною безпекою зазвичай розуміють протидію втраті інформації, доступ до якої обмежений, а також поширенню недостовірної інформації. Однак аналіз відповідних досліджень дозволяє побачити відмінність побутового та наукового підходу до цього поняття. На думку Т.Ю. Ткачук, в юридичній науці серед основних напрямків вивчення питань інформаційної безпеки є визначення головних категорій та понять, що використовуються для регулювання відповідних суспільних відносин [95, с. 20]. Наукові дослідження, предметом яких є проблеми інформаційної безпеки, почали розвиватися на стадії активної інформатизації. Проте це явище існує стільки ж часу, скільки існує людство, проявляючись в різних сферах суспільної діяльності. Проте серед вітчизняних та зарубіжних дослідників немає єдиної загальновизнаної думки навіть щодо самого поняття «інформаційна безпека».

До теперішнього часу було запропоновано багато визначень інформаційної безпеки, але немає єдиної дефініції, що розкривала би сутність досліджуваного феномену. Однією із причин є універсальність цього ключового терміну, що обумовлює необхідність конкретизувати змісту категорії через сфери, через які вона розкривається. Крім того, особливість тлумачення у значній мірі залежить від того аспекту, в межах якого фахівці намагаються дослідити інформаційну безпеку (наприклад, інформаційно-комунікативного, управлінського, правового, технологічного тощо ) [60, с. 16]. У своєму дослідженні Т.Ю. Ткачук для систематизації існуючих визначень пропонує свою класифікацією підходів до визначення інформаційної безпеки у наукових дослідженнях (рис. 1.1).

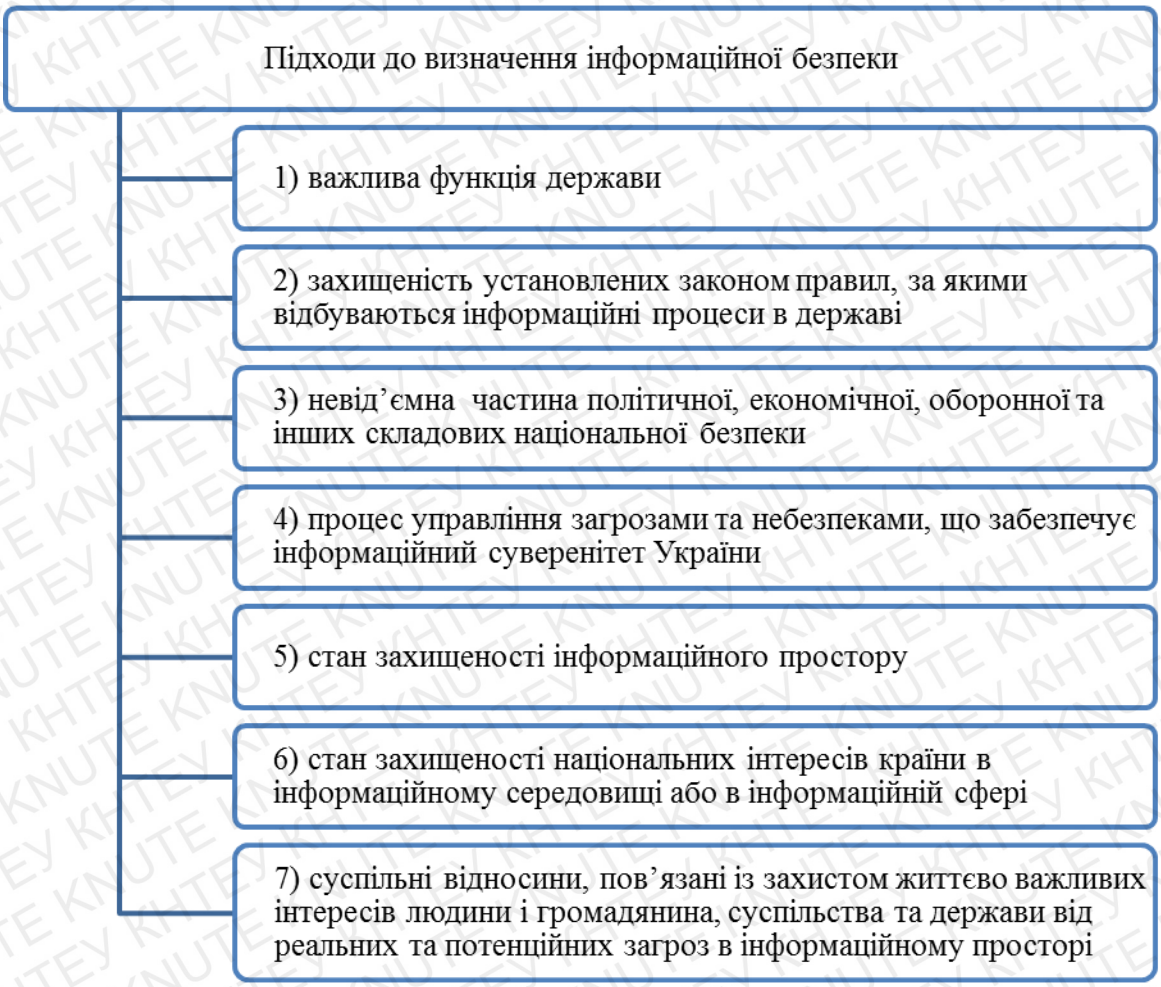


Рис.1.1. Підходи до визначення поняття «інформаційна безпека» [96, с. 63]

За думкою В. Гурковського, інформаційна безпека охоплює суспільні відносини, які пов'язані із охороною життєво важливих інтересів кожної людини або суспільства від реально існуючих або потенційних загроз в інформаційній сфері, що виступають необхідною умовою примноження та збереження духовно-матеріальних цінностей нації, її прогресивного розвитку самозбереження та існування. Одночасно з тим інформаційна безпека стосується України як незалежної держави, яка значною мірою залежить від планомірної інформаційної політики захисту, гарантій та охорони її національних інтересів [69, с. 74].

У свою чергу О. Баранов для визначення інформаційної безпеки застосовує категорію національних інтересів. На думку дослідника, це поняття слід розуміти як стан захищеності національних інтересів держави в інформаційному просторі, що не допускає (або зменшує до мінімуму) завдання шкоди державі, суспільству, людині через несвоєчасність, неповноту, недостовірність чи несанкціоноване

застосування певної інформації, а також через шкідливий інформаційний вплив та наслідки діяльності інформаційних технологій [62, с. 62]. Подібне визначення пропонує В.Т. Шатун, що тлумачить інформаційну безпеку як стан захищеності інтересів держави, окремої особи або суспільства в інформаційному просторі від небезпеки через неповну, несвоєчасну інформацію або її несанкціоноване поширення або використання, від негативного інформаційного впливу та шкідливих результатів функціонування інформаційних технологій [99, с. 175].

Крім того, Р.А. Калюжний визнає, що інформаційна безпека є різновидом суспільних інформаційних відносин у правовій сфері щодо створення, підтримки, захисту та охорони безпечних для людини або суспільства умов життєдіяльності, спеціальних правовідносин, які пов’язані зі створенням, користування зберіганням та поширенням і інформації [74, с. 19].

Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва вважають, що інформаційна безпека це стан правових норм та зв’язаних з ними інститутів безпеки, що дають гарантії постійної присутності даних для прийняття стратегічно важливих рішень та охорони інформаційних ресурсів держави [71, с. 58].

А.Ю. Нашинець-Наумова дотримуються точки зору, що інформаційна безпека являє собою проведення організаційних, правових та інженерно-технічних заходів в процесі використання та формування інформаційних технологій, інформаційних ресурсів та інфраструктури, захист важливої інформації та прав суб’єктів-учасників інформаційній діяльності [84, с.64].

В. Ліпкан, О. Логінов Л. Харченко пропонують тлумачити інформаційну безпеку як процес управління небезпеками та загрозами через державні й недержавні інституції для забезпечення інформаційної незалежності України [78, с. 75].

В.М. Фурашев інтерпретує поняття «інформаційна безпека» як функціонування комплексу засобів, які дозволяють захистити інформаційні системи, що є систематизованою єдністю інформаційних ресурсів (включаючи ресурси держави, юридичних та фізичних осіб), а також інформаційних технологій та системи технічних та програмних засобів, за допомогою яких реалізуються інформаційні процеси в автоматичному або людино-машинному режимі. Формування та

діяльність цього комплексу засобів орієнтоване на гарантування прав як окремої особи, так і в цілому держави та суспільства в інформаційному просторі [97, с. 63]. В.Шульга пропонує тлумачити поняття «інформаційна безпека» за допомогою сукупності таких ознак, як стан, властивість управління небезпеками та загрозами. Перелічені чинники гарантують вибір найліпшого шляху захисту від небезпек та мінімізації дії негативних наслідків, у межах інформаційної сфери держави [100]. Остання дефініція в цілому збігається з точкою зору Р.С. Хаби, котрий інтерпретує поняття «інформаційна безпека» як стан, що відзначається відсутністю загрози, тобто умов та факторів, що є прямою загрозою особі, суспільству або державі у межах комунікаційно-інформаційного простору. Цей підхід сьогодні є найбільш поширеним, та вважається традиційним [98, с. 220].

Проте досить обґрунтованою є позиція І.Ф Корж, що визнає вказану вище постановку питання далекою від реальності, оскільки суспільство у процесі свого розвитку не один раз піддавалося різноманітним негативним впливам (викликам небезпекам, загрозам), яким стає все складніше протидіяти. Одночасно з тим наслідки цих негативних впливів є деструктивними. У зв’язку з цим надмірно сміливо стверджувати про «захищеність» суспільства в інформаційному просторі. У цьому разі доцільніше говорити про певний рівень захищеності, але це ускладнює розуміння досліджуваного явища. На думку дослідника, адекватним та більш наближеним до реальності є підхід, відповідно до якого інформаційна безпека держави – це збалансований стан функціонування інститутів суспільства та держави, за якого гарантується мінімальний вплив деструктивних чинників на національні інтереси держави та її громадян в інформаційній сфері для забезпечення розвитку та формування цієї сфери в інтересах держави, соціуму та людини. Відповідно до наведеного визначення, в інформаційному просторі завжди присутній негативний вплив, що завдає соціуму певної шкоди. Проте, за умови мінімізації цього негативного впливу, можна досягти необхідного рівня функціонування національної інформаційної сфери і його розвитку у майбутньому [76, с. 38].

Важливим кроком на шляху формування системи нормативно-правового регулювання забезпечення інформаційної безпеки України справедливо вважати прийняття Верховною Радою України Конституції України. Цим документом, зокрема, визначені норми, які стосуються забезпечення інформаційної безпеки держави та які є основоположними для побудови національної системи інформаційної безпеки. Категорія «інформаційна безпека» набуває конституційного статусу в нормативно-правовому аспекті відповідно до Ст. 17 Конституції України, яка визначає охорону суверенітету і територіальної цілісності України, а також її економічну та інформаційну безпеку найважливішими функціями держави та справою українського народу [17].

Слід підкреслити, що чинне українське законодавство не містить розгорнутої дефініції інформаційної безпеки. Разом з тим нормативні документи, що стосуються проблем інформаційної безпеки, розглядають її в контексті більш загального терміну «національна безпека». Фактично, в сучасних умовах доступність та наявність інформації про реальний стан та розвиток соціальних економічних, політичних та інших процесів у межах суспільства значною мірою впливають на можливості суспільства в цілому та владних структур щодо прийняття та реалізації ефективних рішень в різноманітних сферах (зокрема, геополітичній, освітній, науковій, культурній та екологічній) [85, с.130].

З іншого боку, інформаційні комунікації та інформація за умов інтелектуалізації та інформатизації суспільства стають рушійною силою, що здатна або забезпечити розвиток та стратегічну стабільність кожній людині та в цілому держави, чи дестабілізувати й роз’єднати суспільство. В умовах розвитку економічної, політичної, оборонної та інших складових національної безпеки певної держави активний розвиток інформаційного простору є важливим фактором життєдіяльності суспільства. Всі ці складові залежать від інформаційної безпеки, а в процесі подальшого розвитку технічного прогресу, ступінь їх залежності тільки зростатиме [68].

Отже, інформаційна безпека являє собою не лише самостійну складову національної безпеки, але також є невіддільною часткою економічної, політичної,

оборонної та інших складових національної безпеки (Додаток А). Спираючись на це припущення, І.Р. Бондар представляє національну безпеку держави в інформаційному просторі як єдність чотирьох складових частин – персональної, суспільної (публічної), корпоративної (комерційної) й державної безпеки). Перелічені типи взаємних відносин між суб'єктами інформаційного суспільства базуються на обміні та використанні інформації. У зв'язку цим, національні інтереси, небезпека для них та управління реальними або потенційними загрозами в межах усіх складових національної безпеки відображаються та реалізуються через інформаційну сферу та інформацію [64, с. 72]. При цьому більш широке поняття «національна безпека» являє собою складне за своєю структурою явище, що включає комплекс умов і чинників охорони національних інтересів, а також процес використання можливостей і ресурсів суспільства для підтримки, збереження та розвитку цих умов і чинників [96, с. 63]

Інформаційна безпека логічно стоїть на першому місці у контексті національної безпеки, виходячи з того, що пріоритет певного виду національної безпеки визначається об'єктивними чинниками: рівнем потреби людей, соціальних груп, суспільства, держав, або в цілому світового співтовариства у безпеці для подальшого розвитку й самозбереження, а також життєво значущих цінностей та об'єктів (соціальних і природних); постійно зростаючою уразливістю суспільства і життєво значущих об'єктів і цінностей (соціальних і природних) без концентрації зусиль на посиленні безпеки; наявністю багатьох надзвичайних загроз, яким система безпеки повинна протидіяти [67, с. 152-153]. Як підкреслює М.М. Присяжнюк, тільки та держава може сподіватися на лідерство в військово-політичній, економічній та інших сферах, мати тактичну та стратегічну перевагу, гнучкіше здійснювати управління економічними витратами на подальший розвиток військової техніки та озброєнь, розвивати передові технології, яка переважає в засобах інформаційної боротьби та інформації. Отже, зміст поняття «інформаційна безпека» в контексті національної безпеки в цілому, доцільно досліджувати з позиції функціонально-діяльнісного підходу, що визначає не як «стан захищеності», а передусім як процес [87, с. 43].

В Україні за роки незалежності були закладені законодавчі основи системи забезпечення інформаційної безпеки, а також була розроблена значна кількість нормативно-правових актів, що визначають головні повноваження державних органів в інформаційній сфері. Чинні акти національного законодавства доцільно розглядати у вигляді 3-рівневої ієрархії (рис. 1.2).

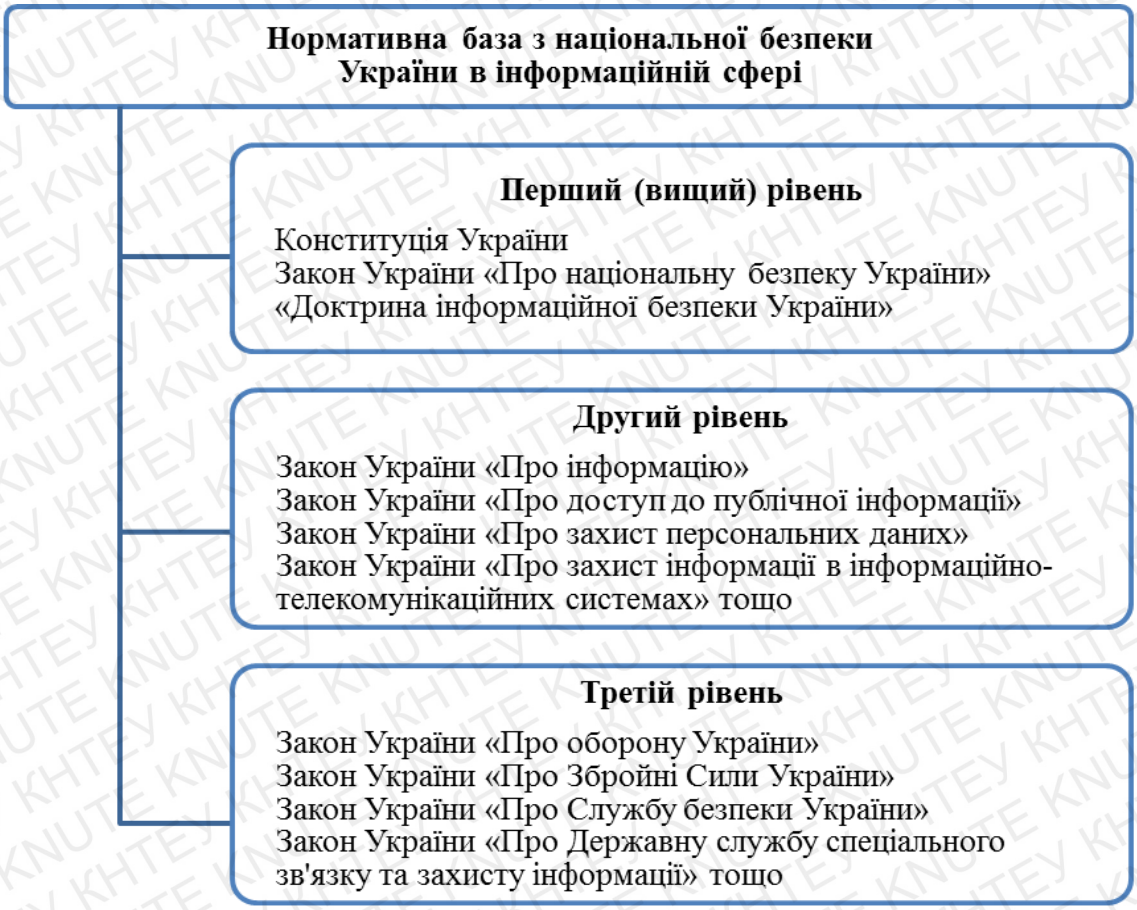


Рис.1.2. Нормативна база з національної безпеки України в інформаційній сфері [81, с. 18-19]

Перший рівень визначає в себе законодавчі акти, що визначають концептуальні положення національної безпеки держави в різних галузях її існування [17; 31; 40]. Другий рівень нормативних актів визначає основні положення забезпечення національної безпеки в інформаційному просторі. Цей рівень містить закони конститутивного напрямку [21; 24; 26; 29; 30 та ін.]. До третього рівня належать нормативні акти, що визначають діяльність державних органів для забезпечення національної безпеки в різних сферах (включаючи й інформаційну сферу). Важливо також додати, що у складі нормативно-правової бази забезпечення національної

безпеки України що стосується в інформаційної сфери особливу роль відіграють розпорядження та укази Президента, а також постанови та декрети Кабінету Міністрів України. Вказані нормативні акти вважаються підзаконними та приймаються для уточнення та покращення якості вирішення актуальних завдань забезпечення інформаційної безпеки в Україні [73, с. 176].

Міністерства й відомства України в межах встановленої законами відповідальності та компетенції на основі чинного законодавства про національну безпеку України, а також відповідно рішенням Кабінету Міністрів та Президента готують положення, відомчі інструкції та накази, що орієнтовані на реалізацію захисту життєво важливих інтересів кожної людини, а також в цілому суспільства та держави в інформаційній сфері. У реалізації державної політики інформаційної безпеки провідну роль відіграє проблема забезпечення балансу між інформаційними свободами людини та необхідністю державного втручання в інформаційні відносини.

Таким чином, узагальнюючи проведений аналіз чинного законодавства України та здобутки провідних дослідників з питань безпеки в інформаційній сфері можна зробити висновки, що інформаційна безпека є не лише самостійною складовою національної безпеки, а й важливою складовою інших сфер національної безпеки держави, спрямованою на забезпечення національних інтересів у цих сферах. Правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України складають: Конституція України, Закон України «Про національну безпеку України» та інші законодавчі та нормативні акти, що регулюють відносини в інформаційній сфері.

## 1.2. Загальноправова характеристика регулювання забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні

Зважаючи на тематику дослідження необхідно, насамперед, визначитися із ключовими термінами та поняттями, що надають змогу охарактеризувати відносини, що виникають у сфері телекомунікацій, зокрема пов'язані з процесами споживання та надання телекомунікаційних послуг. Поміж багатьох термінів першорядну роль відіграють наступні: «телекомунікаційна послуга», «споживач телекомунікаційних послуг», «телекомунікаційна мережа (система)», «телекомунікації» тощо. Задля цього проаналізуємо норми національного та міжнародного законодавства [1; 3; 5; 6; 9; 10; 11; 12; 13; 14; 18; 20; 27; 29; 30; 37; 42 та ін.].

Сутність терміна «Телекомунікаційні послуги» визначена в нормативно-правових документах чинного законодавства України:

1) «послуга – це діяльність виконавця з надання (передачі) споживачеві певного визначеного договором матеріального чи нематеріального блага, що здійснюється за індивідуальним замовленням споживача для задоволення його особистих потреб» [29, п. 13 ч. 1 ст. 1];

2) «телекомунікаційна послуга – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій» [30, ст. 1].

Слід зазначити, що зміст другої дефініції є досить абстрактним через використання невизначених законодавчо формулювань «потреб споживачів у сфері телекомунікацій» та «продукту діяльності». У зв'язку з цим доцільно звернутися до ключових положень загальноєвропейських юридичних тлумачень телекомунікаційних послуг:

1) під ними розуміються послуги, що зазвичай постачаються за певну плату, «… які полягають повністю або головним чином у передачі сигналів по електронних комунікаційних мережах» [11, п. с ч. 1 ст. 2; 14, п. 3 ч. 1 ст. 1];

2) до них не відносяться «… послуги, що здійснюються, або надаються поза редакторським наглядом змісту…» з боку споживача: «продаж пакетів із телевізійним або звуковим змістом мовлення», «постачання змісту, основою якого є технології WWW», «певні послуги інформаційного суспільства та фінансові послуги» тощо [3; 14, п. 3 ч. 1 ст. 1; 245, п. с ч. 1 ст. 2]. Отже, у законодавчій практиці країн ЄС застосовується принцип точного розмежування між «регулюванням передачі та регулюванням змісту», що знаходить закріплення в офіційному тлумаченні телекомунікаційних послуг [11, п. с ч. 1 ст. 2; 14, п. 3 ч. 1 ст. 1]. Інакше кажучи, законодавство чітко розділяє телекомунікаційні послуги та інформаційні послуги.

В ході виконаного дослідження вітчизняної правової бази стає очевидною відсутність норм, що точно дають визначення та конкретизують складові поняття «телекомунікаційна послуга». Ця ситуація наочно демонструє загальновідому як правознавцям, так і технічним фахівцям, проблему термінології в сфері телекомунікацій. У зв’язку з цим досить обґрунтованою є позиція Д.В. Сулацького, який визнає необхідність більш детального вивчення технічних та організаційних аспектів надання телекомунікаційних послуг для розробки оптимальної дефініції. Крім того, дослідник зауважує, що в межах окремого наукового дослідження складно охарактеризувати всі існуючі на сьогодні телекомунікаційні послуги та пов’язані з ними технології. Одночасно з цим важливо враховувати швидкий технологічний прогрес та постійний розвиток в інформаційно-телекомунікаційній галузі, що є причиною розробки та впровадження у життя нових продуктів [92, с. 76].

За таких обставин найбільш логічним вирішенням визначеної проблеми є виділення для опрацювання найбільш загальнодоступних та поширених сучасних телекомунікаційних послуг, що визначені чинним законодавством, та подальшому розв’язанні на цій основі визначених на початку роботи дослідницьких задач.

У відповідності до чинних «Правил надання та отримання телекомунікаційних послуг» телекомунікаційні послуги поділяються на загальнодоступні (універсальні) та інші телекомунікаційні послуги. Крім того, телекомунікаційні

послуги поділяються на основні та додаткові за характером надання, що технологічно відповідає наданим основним телекомунікаційним послугам. До реєстру додаткових належать послуги, обумовлені технічними можливостями використовуваного операторами та провайдерами телекомунікацій обладнання [44, п. 3].

Сутність поняття «телекомунікації» в сучасних умовах достатньо точно розкривається в положеннях чинних правових норм:

1) телекомунікації – це передавання, приймання та/або випромінювання сигналів, знаків, письмового тексту, звуків та зображень або повідомлень будь-якого роду по проводових, радіо, оптичних та інших електромагнітних системах [30, ст. 1];

2) телекомунікації являють собою невід'ємну частину соціальної та виробничої інфраструктури держави, що використовуються для задоволення потреб юридичних та фізичних осіб, а також органів державної влади в телекомунікаційних послугах [30, ст. 3];

3) телекомунікації – це складова глобальної інформаційної інфраструктури, що за принципами побудови забезпечує вільний рух інформації між її численними інформаційно-спеціалізованими складовими, такими як споживачі інформації та джерела, бази даних та сховища, розповсюджувачі інформації та переробники тощо» [45, розділ 4].

Досліджуване питання також можна доповнити законодавчим тлумаченням «електронної комунікації», що використовується в Європейському Союзі та означає будь-яку інформацію, яку передають або обмінюються між певною кількістю сторін за допомогою публічно доступних послуг електронних комунікацій. Це не стосується будь-якої інформації, що передається у якості послуги телерадіомовлення для аудиторії за допомогою мережі електронних комунікацій (виключенням є ті випадки, коли інформація має відношення до користувача або абонента, яких можуть бути ідентифіковані та отримують інформацію [9, п. d ч. 2 ст. 2].

Поряд із цим, цілком поміркованим і прийнятним у контексті проблематики даного

дослідження є наступне вітчизняне нормативне визначення телекомунікації як випромінювання, передавання або/та приймання сигналів, знаків, письмового тексту, звуків, зображень або повідомлень будь-якого роду, що передаються за допомогою проводових, радіо, оптичних або інших електромагнітних систем [30, ч. 1 ст. 1; 44, п. 3].

Відповідно до визначення законодавства Європейської Спільноти під телекомунікаційними мережами (системами) розуміються «… системи передачі, включаючи за потреби маршрутизатори, комутаційне обладнання або інші ресурси, які дають змогу а також сигналів по дротах, через радіо, оптичні та інші електромагнітні засоби, включаючи мережі супутникового зв'язку, виділені мережі, (мережу з комутацією каналів та пакетів, в тому числі Інтернет), електричні кабельні системи та глобальні мережі мобільного зв'язку, якщо вони застосовуються з метою передачі сигналів, мережі, що використовуються для теле- та радіомовлення, а також мережі кабельного телебачення, незалежно від типу інформації, яка передається [11, ч. 1 ст. 2; 14, ч. 1 ст. 1].

Щодо нормативного роз'яснення досліджуваної категорії в національному законодавстві, пріоритет якого для дослідження є безумовно вищим, то тут мають місце певні понятійні неузгодженості. Тому говорячи про інформаційну, телекомунікаційну та інформаційно-телекомунікаційну систему чи мережу, у подальшому доцільно використовувати узагальнюючий термін «інформаційно-телекомунікаційна система». В свою чергу, тлумачення останньої базується на положеннях Законів України «Про телекомунікації» та «Про захист інформації в інформаційно-телекомунікаційних системах» стосовно тлумачення понять «телекомунікаційної системи», «телекомунікаційної мережі», «інформаційної системи» та «інформаційно-телекомунікаційної системи» [30, ч. 1 ст. 1].

Доцільно відзначити, що на теперішньому етапі науково-технічного розвитку запропоноване термінологічне утворення носить практично універсальний характер. Однак ним не охоплюються тільки поодинокі варіанти реалізації телекомунікаційної чи інформаційної системи, зокрема:

1) випадок окремо встановленого персонального комп'ютеру, який відокремлений від яких-небудь телекомунікацій (відсутнє з'єднання з локальною комп'ютерною мережею тощо);

2) випадок розбудови ізольованої мережі радіо- або провідного зв'язку виключно на основі електромеханічного, аналогового обладнання (комутаторів, польових телефонних апаратів тощо) [92, с. 75].

До розгляду питань законодавчого тлумачення понять «споживач телекомунікаційних послуг», «оператор телекомунікацій» і «провайдер телекомунікацій» в Україні доцільно підійти на основі узагальнюючого дослідження положень національних нормативно-правових актів [18; 20; 29; 30; 44]. Перш за все необхідно підкреслити, що правова основа діяльності у сфері телекомунікацій встановлена Законом України «Про телекомунікації», яким визначаються повноваження держави щодо відповідальності юридичних та фізичних осіб, що користуються телекомунікаційними послугами або беруть участь у даній діяльності [30]. Крім того, «Правилами надання та отримання телекомунікаційних послуг», що затверджені Постановою Кабінету Міністрів України, визначається порядок надання, регулювання та управління даної діяльності, а також обов'язки, права та основні засади отримання телекомунікаційних послуг (у рамках телекомунікаційних мереж загального користування), регулюють відносини між споживачами телекомунікаційних послуг, а також провайдерами та операторами телекомунікацій [44, п. 1, п. 2].

Разом з тим «Правилами надання та отримання телекомунікаційних послуг» встановлюється, що на території України надання телекомунікаційних послуг є виключним правом:

1) юридичних осіб з місцезнаходженням на території України, які зареєстровані у відповідності до чинного законодавства України

2) фізичних осіб, що є суб'єктами підприємницької діяльності та мають на території України постійне місце проживання [44, п. 5].

Також «Правилами надання та отримання телекомунікаційних послуг» встановлено, що в Україні телекомунікаційні послуги можуть надаватися на умовах

договору між споживачем телекомунікаційних послуг та оператором (провайдером) телекомунікацій або без такого у випадку одержання споживачем замовленої за попередньою оплатою послуги). Розрахунки за послуги можуть здійснюватися за допомогою телекомунікаційних карток або за готівкову оплату [44, п. 34, п. 35]. Відповідно до Закону України «Про захист прав споживачів» відбувається регулювання відносини між споживачами послуг та надавачами послуг, встановлюються права споживачів телекомунікаційних послуг, встановлюються основи реалізації державної політики у сфері захисту прав споживачів, а також визначається механізм захисту інтересів споживачів [29].

Положення Господарського кодексу України розкривають головні засади господарювання в Україні і регулюють господарські відносини, які виникають між суб'єктами господарювання у процесі здійснення та організації господарської діяльності, а також між цими суб'єктами та іншими учасниками відносин у сфері господарювання (зокрема, споживачами, органами місцевого самоврядування та органами державної влади, що наділені господарською компетенцією, а також організаціями та громадянами) [18, ч. 1 ст. 1, ст. 2]. Встановлені у Цивільному кодексі України норми регулюють особисті майнові та немайнові відносини (цивільні відносини на принципах вільного волевиявлення, юридичної рівності та майнової самостійності їх учасників: фізичних та юридичних осіб, територіальних громад, держави, іноземних держав, а також інших суб'єктів публічного права [20, ч. 1 ст. 1, ст. 2].

Таким чином, визначені в національному законодавстві ключові поняття у сфері телекомунікацій за своєю сутністю практично співпадають із трактуваннями відповідних юридичних категорій міжнародних установ та є цілком раціональними та прийнятними для подальшого дослідження в контексті даної роботи.

Засновуючись на аналізі нормативно-правової бази та науково-практичної літератури достатньо обґрунтованою видається запропонований Д.В. Сулацьким об'єктно-суб'єктний склад інформаційної безпеки в сфері телекомунікацій, в основу якого покладено специфічні риси об'єктів та суб'єктів інформаційних

відносин. В контексті безпеки споживання телекомунікаційних послу дослідник пропонує наступний склад інформаційної безпеки (рис.1.3)

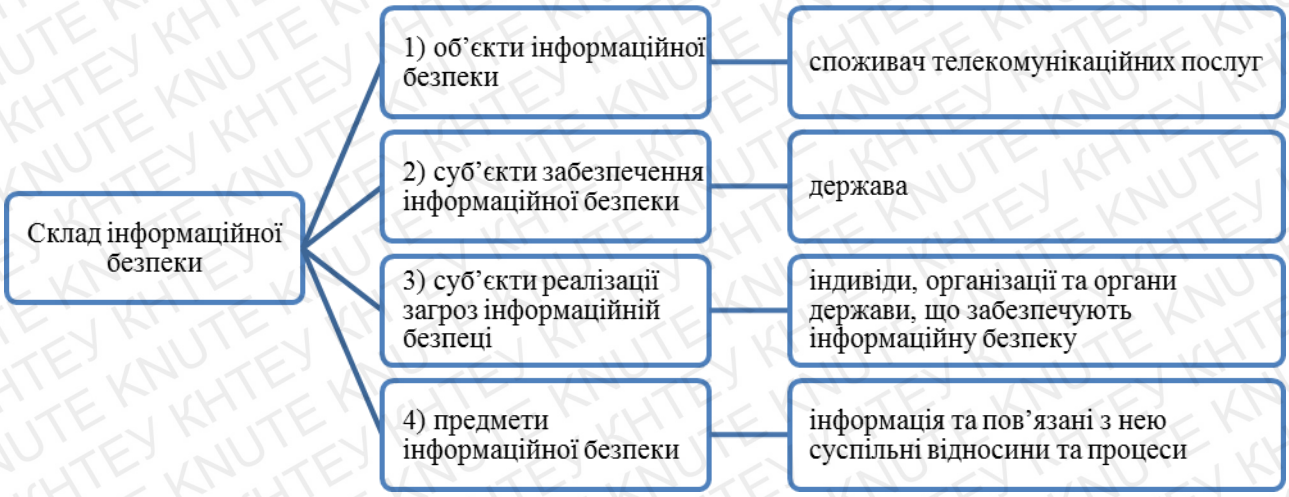


Рис. 1.3. Об'єктно-суб'єктний склад інформаційної безпеки [92, с. 86-88]

На думку Д.В. Сулацького, зазначені на схемі (рис. 1.3) суб'єкти та об'єкти виступають фактичними учасниками суспільних відносин в сфері телекомунікацій, але вони не отримали відповідного нормативно-правового врегулювання. Даний факт може бути інтерпретований як одне із джерел загроз інформаційній безпеці людини, що виступає споживачем телекомунікаційних послуг. Інакше кажучи, забезпечення цієї безпеки ототожнюється з виявленням виявлених юридичних прогалин та розробкою організаційно-правових засад стосовно їх нейтралізації в Україні [92, с. 88].

Таким чином, у контексті даної роботі держава розглядатиметься не тільки як суб'єкт забезпечення, але й як опосередкований суб'єкт реалізації загроз інформаційній безпеці споживача телекомунікаційних послуг в Україні. Зауважимо, що відповідно до вищевикладених міркувань склад новоутвореної групи суб'єктів можна розширити, зокрема, включивши до неї оператора чи провайдера телекомунікацій, які, користуючись прогалинами в чинному законодавстві, не забезпечують інформаційну безпеку власних абонентів на достатньому рівні.

## 1.3. Зарубіжній досвід правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг

Глобальна природа сучасної інформаційної сфери із недосконалим механізмом ідентифікації окремих користувачів та неможливістю завжди встановити місце їх перебування та наслідки дій сприяють зростанню міжнародній злочинності та негативно впливають на стабільний розвиток сучасного міжнародного суспільства, що, у свою чергу, є основою економічного розвитку та процвітання кожної людини. Перелічені фактори відображають уразливість національних та міжнародних інформаційних інфраструктур, в межах яких особливо актуальною стає безпека споживачів комунікаційних послуг. У зв'язку з цим на сучасному етапі забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг, та зокрема її правовий аспект, перебуває на стадії становлення на національному рівні [87].

Недовершеність правового аспекту регулювання відносин в інформаційній сфері заважає вдосконаленню та нормальному розвитку інших відносин у суспільстві (наприклад, економічних, політичних, матеріальних), а також процесу забезпечення інформаційної безпеки країни [83, с. 105]. Слід підкреслити, що наша держава не першою зіштовхнулася з проблемою забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг. Досліджувана проблема успішно вирішується в країнах, що є членами Європейського Союзу та Північноатлантичного Альянсу. Практика нормативно-правового регулювання суспільних відносин у сфері захисту прав споживачів телекомунікаційних послуг з точки зору інформаційної безпеки в цих країнах робить доцільним більш детальне вивчення зарубіжного досвіду.

Найбільш розвинутим законодавством, що стосується інформаційної безпеки, вважається система США. У цій державі процес створення законодавчих актів відбувався цілеспрямовано, відповідно до виникаючих проблем. Взагалі кількість законодавчих актів досягає кількох сотень. З іншого боку, в європейських країнах ведеться не менш інтенсивна в робота в цьому напрямі. Слід підкреслити, що в 1949

році на початку діяльності НАТО суттєво відрізнялися системи безпеки країн-учасниць. На сучасному етапі діють стандарти НАТО стосовно захисту інформації, закріплені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)» [109]. Крім того, спеціальним документом закріплена офіційна політика організації щодо кіберзахисту [115; 118], а також стратегічна концепція кібербезпеки, визначена за результатами Лісабонського саміту [116] та передбачені за результатами Варшавського саміту [117] тощо.

Необхідно підкреслити, що першорядним завданням НАТО є запобігання випадків агресії у кіберпросторі [110], адже кібератаки стають усе більш частими, збитковими та організованими для об'єктів критичної інфраструктури, державних установ, організацій, а також можуть сягнути критичного рівня, який буде загроджувати національному та євроатлантичному розвитку, стабільності та безпеці всього міжнародного співтовариства. Основним джерелом таких атак можуть бути організовані злочинні угруповання, іноземні розвідувальні або військові служби, екстремістські або терористичні угруповання [118].

У сфері кіберзахисту офіційна політика НАТО (NATO Cyber Defence Policy) була схвалена міністрами оборони держав-членів і представлена учасникам організації у квітні 2008 р. на саміті в Бухаресті. Головною метою цього документу є забезпечення можливості для надання підтримки країнам-союзницям, на їх вимогу, у протидії кібератаці [115]. У Декларації Лісабонського саміту та у Стратегічний концепції зазначено, що постійне ускладнення та швидкий розвиток кібернападів роблять захист інформаційно-комунікаційних систем країн-членів НАТО таким, від якого залежить майбутня безпека на рівні організації, а інформаційні атаки фігурують серед найнебезпечніших викликів і загроз безпеці та процвітанню держав-членів Альянсу [116].

На сучасному етапі в зазначених країнах ЄС існує ряд викликів безпеці інформаційних інфраструктур, що охоплюють:

1) відсутність координованих внутрішньодержавних підходів до безпеки інформаційної сфери, що зменшує рівень ефективності національних заходів;

2) недостатній розвиток на міжнародному рівні партнерства між приватним та державним секторами;

3) обмеженість можливостей стосовно раннього реагування та попередження на безпекові інциденти, спричинені нерівномірним розвитком систем контролю та сповіщення про випадки у інших країнах, а також нерозвиненість міждержавного обміну інформацією та співробітництва стосовно цих проблем;

4) недосконаліть міжнародного співробітництва відносно пріоритетних напрямків у реалізації політики захисту важливої інформаційної інфраструктури [107].

Наразі в країнах ЄС до числа стратегічних пріоритетів національної безпеки належить вирішення питань, пов'язаних з забезпеченням інформаційної безпеки держави, суспільства та людини, а також їх захист від зовнішніх та внутрішніх загроз в сфері комунікаційних послуг. Одночасно з тим країни-члени Європейського Союзу втілюють у національній політиці забезпечення інформаційної безпеки стандарти, що уточнені у наступних нормативно-правових актах:

- «Європейськими критеріями безпеки інформаційних технологій» (1991 р.) [113];
- «Єдиними критеріями безпеки інформаційних технологій» (1996 р.) [105];
- «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.) [108];
- «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (2007 р.) [106] тощо.

Одним з найбільш важливих питань політики інформаційної безпеки країн-членів ЄС є захист персональних даних споживачів комунікаційних послуг. У цьому випадку діють положення Директиви 95/46/ЄС «Про захист фізичних осіб у зв'язку з обробкою персональних даних і вільного обігу таких даних» [7]. У відповідності до цього нормативного документа одночасно затверджується прагнення до вільного обміну інформації між країнами та надаються гарантії захисту основних

прав громадян, до яких входить право на недоторканність особистих даних і їх захист від третіх осіб. Разом з тим з 2016 року на території країн-членів ЄС, набули чинності нові правила захисту персональних даних (GDPR – Загальний Регламент щодо захисту персональних даних), які поширюються як на європейські компанії, так й на компанії з інших країн, які пропонують телекомунікаційні послуги в ЄС. Для Ірландії, Фінляндії та Австрії нові правила набули чинності у 2018 році. У даному документі вказуються цивільні права користувачів телекомунікаційних послуг, відповідальність сторін за безпеку даних, а також виділені певні обмеження обміну даними в межах різних країн. Серед важливих нововведень є застосування суворішого покарання за невчасне повідомлення інформації щодо виток даних. Для компаніям, які не доповіли про факт злому або витоку інформації продовж 72 годин з моменту виявлення такої події та порушили положення нової директиви, передбачений штраф, що сягає до 20 млн. євро або до 4% річного доходу [112].

Крім того, у вказаній вище Директиві передбачена необхідність отримати згоду користувачів комунікаційних послуг на обробку їх персональних даних (зокрема, на обробку даних з різними цілями надається окрема згода). Нормативний акт встановлює, що згода повинна бути конкретною, свідомою та вільною, та може бути відкликана людиною в будь-який час. Згода не вважається вільною, якщо користувач змушений дати свою згоду для отримання доступу до певної програми, додатка або сайту. До виключних випадків належать ситуації, коли персональні дані користувача необхідні для виконання певної угоди. У тих випадках, коли персональні дані обробляються або збираються з метою подальшого маркетингового аналізу, користувач має можливість відмовитись надавати свої данні для подальшої обробки. Компанії, що надають комунікаційні послуги та отримують та оброблюють персональні дані, також обов’язково:

- ведуть облік операцій з персональними даними (зокрема, тип даних і ціль, для якої вони обробляються);
- мінімізують використання персональних даних;
- проводять внутрішній аудит [112].

У межах даної роботи також вважається доцільним охарактеризувати досвід забезпечення безпеки в інформаційній сфері європейських країн, які не є зараз членами НАТО, однак є членами ЄС, на прикладі Фінляндії, Ірландії та Австрії. Насамперед необхідно зауважити, що членство в ЄС накладає на ці країни обов'язки стосовно дотримання діючих стандартів цієї організації щодо забезпечення інформаційної безпеки та розвитку інформаційного суспільства. Для цього в 1991 році був розроблений спеціальний документ «Європейські критерії безпеки інформаційних технологій», в якому визначені наступні завдання забезпечення інформаційної безпеки:

- захист від несанкціонованого доступу інформаційних ресурсів для забезпечення конфіденційності;
- забезпечення цілісності інформаційних ресурсів через їх захист від знищення або несанкціонованої модифікації;
- забезпечення працездатності систем через протидію загрозам відмови в обслуговуванні [113].

Як і в інших країнах ЄС, в Австрії, Фінляндії та Ірландії, значна увага приділяється питанням безпеки у кіберпросторі, що були окреслені у Документі Європейської комісії «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», де остання визначена як кримінальна дія, вчинена з вживанням інформаційних систем, електронних комунікаційних мереж або проти вказаних систем та мереж [106].

Треба підкреслити, що за показниками розвитку інформаційного суспільства Фінляндію вважають одним із лідерів ЄС, оскільки в рейтингу країн Євросоюзу вона утримує першість за рівнем цифрової грамотності й посідає друге місце за показником поширення мережі широкосмугового зв'язку [92, с. 256]. Головними державними інституціями, відповідальними за реалізацію та розробку політики інформаційної безпеки, виступає Міністерство транспорту та комунікацій Фінляндії. До повноважень цього державного органу входить розробка законодавства стосовно безпеки даних, комунікаційних мереж, забезпечення доступу до комунікаційних послуг, а також реалізація та розробка національної політики у сфері інформаційної безпеки. Важливим структурним підрозділом

Міністерства є Управління Фінляндії з регулювання комунікацій (FICORA), до компетенції якого входить державне регулювання та контроль у сфері інформаційно-комунікаційних технологій. До повноважень FICORA належить:

- контроль за функціонуванням електронних комунікаційних мереж;
- підвищення обізнаності громадян з питань інформаційної безпеки;
- планування й управління використанням радіочастот, мережевими адресами, а також контроль за змістом програм і реклами на телебаченні та радіо;
- інформування про можливі загрози інформаційній безпеці [104].

Щодо Австрійської Республіки, то в цій країні програми становлення інформаційного суспільства втілюють політичну стратегію об'єднання Європи на базі новітніх технологій, інтелектуального потенціалу регіону та інформаційно-комунікаційної інфраструктури. Значний вплив на інформаційну політику та безпеку у комунікаційних мережах країни чинять міжнародні організації, що у Відні мають резиденції, складовою програм діяльності яких є розвиток інформаційного суспільства. Головним пріоритетом Австрії є забезпечення інформаційної безпеки на національному й міжнародному рівнях. Всеосяжна політика інформаційної безпеки означає, що внутрішня та зовнішня безпека, а також різні аспекти військової та цивільної безпеки взаємозалежні та тісно пов'язані [103].

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

надійне й послідовне реагування як на національному, так і на міжнародному рівні [114].

Виняткове місце серед країн позаблокового статусу займає Швейцарія, що не є ані членом НАТО, ані ЄС. З 1992 року у Швейцарії діє Федеральний акт про захист даних, який дозволяє втілювати загальноєвропейські принципи захисту інформації, в тому числі персональних даних користувачів комунікаційних мереж [111]. Верховний суд Швейцарії у 2010 році надав додаткові гарантії конфіденційності персональних даних та підтримав місцевого уповноваженого із захисту таких даних. Зокрема, був ухвалений порядок, у відповідності до якого визнаний незаконним збір інформації про IP-адреси користувачів файлообмінних мереж без їхньої згоди [66].

Таким чином, головними напрямами забезпечення інформаційної безпеки у розглянутих країнах НАТО та ЄС є наступні:

1) правове забезпечення інформаційної безпеки, в межах якого перевага надається захисту персональних даних, регулюванню телекомунікаційних послуг та перешкоді кіберзлочинності;

2) організація спеціальної європейської системи, що орієнтована на своєчасне інформування та попередження користувачів телекомунікаційних послуг про нові загрози;

3) покращення обізнаності користувачів щодо потенційних загроз під час використання телекомунікаційних мереж;

4) зміцнення технологічної підтримки;

5) розвиток міжнародного співробітництва, направленого на вирішення питань інформаційної безпеки.

**Висновки**

В умовах глобалізації інформаційного суспільства телекомунікації виступають головним чинником зростання інформаційних небезпек для людини. У такій ситуації держава виконує провідну роль у протидії інформаційним небезпекам для людини, яка є споживачем комунікаційних послуг, у процесі забезпечення інформаційної складової національної безпеки – інформаційної безпеки. Забезпечення безпеки в телекомунікаційній сфері суттєво залежить від якісного правового регулювання цих інформаційних правовідносин.

Активну політику у напряму забезпечення інформаційної безпеки проводить не тільки НАТО, але й країни ЄС, що об'єднує економічно розвинуті країни та значною мірою впливає на міжнародні відносини, визначаючи стандарти та норми поведінки країн, перш за все, у соціальній, економічній, політичній та інформаційній сфері. Вивчення практики європейських країн у формуванні власних моделей правового забезпечення інформаційної безпеки, а також аналіз діючих у рамках міжнародної спільноти правових документів дає змогу зробити висновок про відсутність єдиної моделі національної системи правового забезпечення інформаційної безпеки. Фундаментальними принципами реалізації державної політики в указаній сфері є дотримання балансу між інтересами окремої людини, суспільства та держави, що забезпечується шляхом законодавчого регулювання реальних і прозорих механізмів їх взаємної відповідальності та контролю.

Небезпеки у телекомунікаційному просторі доволі результативно опрацьовані та активно вивчатися з позицій різних наук, у їх числі й юридичних, а також знайшли своє закріплення у національному та міжнародному законодавстві. Ґрунтуючись на теорії правовідносин, що розробляється фахівцями у галузі теорії держави і права, в роботі доведена необхідність дослідження та виокремлення в структурі інформаційних правовідносин нового предмета – відомостей, які водночас запропоновано розглядати як предмет безпеки.

# РОЗДІЛ 2
# УДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ НАДАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ В УКРАЇНІ

## 2.1. Стан забезпечення інформаційної безпеки людини в Україні як споживача телекомунікаційних послуг

Дослідження організаційно-технічних засад функціонування та побудови систем чинного законодавства України у сфері телекомунікацій дозволяє виділити можливості надання послуг телефонії через використання:

- фіксованого зв'язку із застосуванням нерухомого (стаціонарного) кінцевого обладнання, або за допомогою безпроводового доступу до системи [39, ч. 1 ст. 1, ч. 3 ст. 42];
- рухомого (мобільного) зв'язку, що здійснюється за допомогою радіотехнологій, коли кінцеве обладнання споживача послуг (далі – термінал) може переміщатися вільно в межах діючих пунктів закінчення системи та зберігає єдиний ідентифікаційний номер, що є унікальним [47, п. 1.7-1.9].

Зважаючи на тему дослідження, доречним постає паралельний аналіз:

1) процесів споживання (надання) розглянутих вище послуг;
2) особливостей функціонування підрозділів операторів телекомунікацій, які здійснюють діяльність з надання послуг рухомого зв'язку (далі – оператори);
3) законодавчого регулювання у сфері телекомунікацій України.

Системами операторів оброблюється певний набір відомостей щодо наданих споживачам послуг (далі – відомостей), які можна визначити та класифікувати за критерієм їх призначення:

1) розрахункові дані – відомості, на основі яких системами операторів здійснюється облік наданих послуг і наступні розрахункові операції з абонентами;
2) службові дані – відомості суто технічного характеру, що забезпечують функціонування систем операторів і терміналів щодо надання та споживання послуг, підтримки з'єднання тощо [20, ст. 257].

Серед розрахункових даних слід виділити інформацію про:

- абонентські номери (MSISDN), що беруть участь у отриманні послуг;
- час початку, завершення та тривалість з'єднання, надання послуги;
- вид послуги, напрям з'єднання;
- телекомунікаційні картки, що використовувалися для розрахунків із оператором [50, п. 3.21].

Стосовно розрахункових даних потрібно додати, що облік відомостей цього виду в тому чи іншому обсязі ведеться всіма операторами рухомого (мобільного) та фіксованого зв'язку. В свою чергу, системи операторів можуть бути побудовані на різноманітній технологічній базі, що обумовлює відмінність між службовими даними. До основних службових даних рухомого зв'язку віднесемо інформацію про міжнародний ідентифікаційний номер рухомого абонента (IMSI), міжнародний ідентифікаційний номер терміналу (IMEI) та постійне місцезнаходження споживача відносно підсистеми базових станцій (BSS) оператора. Однак наведена класифікація відомостей має певною мірою гнучку природу. Наприклад, інформацію про абонентські номери можна одночасно віднести як до розрахункових даних, так і до службових, адже вони безпосередньо необхідні для встановлення з'єднання між абонентами. Аналогічно, такий різновид службових даних, як місцезнаходження споживача в системі оператора може впливати на вартість послуг [50, 3.21, п. 4.4.2].

Враховуючи вищевикладене та наявну професійну термінологію оперативних підрозділів і операторів у ході дослідження використовуватиметься відповідна класифікація вибірок службових і розрахункових даних. Вибірки стосовно одного конкретного споживача (за абонентським номером, міжнародним ідентифікаційним номером терміналу, номером особистого рахунку, номерами використаних телекомунікаційних карток тощо) найчастіше називають «деталізація з'єднань абонента» або «деталізація телефонних переговорів абонентського номеру». Типовою формою подання таких вибірок є табличний вигляд, що складається з певного набору стовпців, кожний з яких містить той чи інший різновид службових або розрахункових даних [63, с.11-12; 75, с. 26].

Працівники операторів у тому чи іншому обсязі мають доступ до інформації про переміщення, особисті зв'язки (контакти) абонентів в процесі виконання своїх службових обов'язків. Наявність доступу обумовлює можливість умисної або неумисної передачі відомостей стороннім зацікавленим особам. Крім того, збір та аналіз моніторингів та деталізацій дають можливість встановлювати постійний контроль за основними аспектами приватного життя кожного споживача, чи їх групи без залучення жодних технічних засобів розвідки [70; 75 с. 10-11; 77 с. 16-17; 88, п. 2.10; 90; 94, с. 70-71]. Даний факт може бути розцінений як прояв розвідувальної роботи, тобто наявну загрозу, ризик якої прямо пов'язаний із зростанням інтенсивності споживання телекомунікаційних послуг. Така ситуація дає підстави для виділення у рамках даної роботи в якості предмета безпеки саме вищезгадані відомості. На наступних етапах дослідження необхідно зосередитись на докладному вивченні пов'язаних із ними суспільних відносин. У відповідності до обраного напряму подальшого дослідження логічно постає питання про вивчення стану забезпечення інформаційної безпеки людини з точки зору доступу оперативних підрозділів до відомостей та їх вибірок.

Необхідно зазначити, що відповідно до вимог національного законодавства у сфері телекомунікаційних послуг оператори зобов'язані надавати інформацію щодо споживачів та наданих їм комунікаційних послуг лише в порядку та у випадках, визначених діючим законодавством, або ж за наявністю письмової згоди споживача [30, ч. 3 ст. 34, ч. 2 ст. 39]. Крім того, в національному законодавстві активно використовуються фактично тотожні за своєю сутністю в контексті змісту розглянутих норм терміни: «інформація про надані телекомунікаційні послуги», «відомості щодо наданих телекомунікаційних послуг», «інформація про з'єднання… абонента», «рахунки за надані телекомунікаційні послуги», «записи про надані телекомунікаційні послуги», , «дані обліку телекомунікаційних послуг» тощо. Однак у законодавчих актах відсутня систематизації вказаних понять не формулюється. Присутня лише розосереджена конкретизація дефініції відомостей у значенні розрахункових даних стосовно віднесення до них зведень щодо «…номера абонента, якого викликав споживач, виду послуги, часу початку і

закінчення кожного сеансу зв'язку, обсягу наданих послуг, суми коштів до сплати за кожний сеанс зв'язку», самих фактів «… отримання послуг, їх тривалості, змісту, маршрутів передавання тощо» [30, п. 16 ч. 1 ст. 32, ч. 1 ст. 34; 47, п. 4.1.19].

З іншого боку, в межах дослідження слід відзначити такі збіжні нормативні терміни як «відомості щодо змісту наданих телекомунікаційних послуг», «інформація щодо змісту телекомунікаційних послуг» та «відомості про зміст наданих телекомунікаційних послуг». Перелічені терміни породжують деякі смислові паралелі із поняттям змісту самого телекомунікаційного повідомлення, тобто «змістом інформації, що передається або приймається споживачем (абонентом)», або ж «змістом інформації, що передається телекомунікаційними мережами». Однак зміст даної інформації оператор уже не має права контролювати та не несе за нього відповідальності [12, ч. 4 ст. 40]. У зв'язку з цим законодавцем передбачено двоякий характер розуміння категорії «змісту» стосовно сфери надання телекомунікаційних послуг, що породжує неоднозначність тлумачення відповідних правових норм. Підсумовуючи наведені результати дослідження, можна зазначити, що відсутність у національному законодавстві чіткої дефініції та класифікації відомостей породжує сприятливі передумови для безперешкодної реалізації відповідних загроз і може розцінюватися в якості їх загального джерела. Також чинне законодавство вказує на такий аспект безпеки, як «схоронність відомостей щодо споживача, отриманих при укладенні договору» (наприклад: прізвище, ім'я та по батькові, місце проживання, абонентський номер чи номер телефону, поштова чи електронна адреса доставки тощо). Фактично мова йде про захист персональних даних абонентів. Однак, у даному дослідженні зазначена проблематика не буде розроблятися. Вона певним чином уже знайшла своє правове врегулювання в Україні та не носить надзвичайно актуального характеру для нашої країни, оскільки абсолютна більшість українських абонентів рухомого зв'язку отримує послуги без реєстрації в оператора своїх персональних даних [2; 16; 17, ст. 32; 28; 30, ст. 23; 39, п. 16 ч. 1 ст. 32].

Несанкціонований доступ до змісту інформаційного (телекомунікаційного) повідомлення можна вважати порушенням таємниці телефонних розмов,

листування, телеграфної або іншої кореспонденції, які передаються через комп'ютер або іншими засобами зв'язку [19, ст. 163]. В умовах глобалізації телекомунікаційної сфери оперативні підрозділи для результативного виконання своїх зобов'язань перед особою, суспільством і державою потребують використання деталізацій і моніторингів як нового інформаційного джерела при документуванні протиправної (злочинної) діяльності, розкритті правопорушень і розшуку правопорушників, а не тільки виступають суб'єктами загроз, реалізація котрих зумовлена доступом до службових і розрахункових даних. На законних підставах вітчизняні оперативні підрозділи мають право витребувати у компаній-операторів мобільного зв'язку наступну інформацію:

1) відомості , що стосуються осіб, котрі підозрюються у вчиненні злочину;
2) відомості, необхідні для встановлення істини у кримінальній справі;
3) відомості, які потрібні для розслідування, розкриття, попередження злочину [34, п. 11 ч. 1 ст. 8].

Практика доступу оперативних підрозділів до відомостей щодо наданих телекомунікаційних послуг постійно змінювалась (див. Додаток Б). Існуюче в українській правозастосовній практиці попереднє погодження з прокуратурою та судове санкціонування доступу вказаних підрозділів до службових і розрахункових даних без негласного застосування спеціальних технічних засобів вважається декотрими дослідниками дещо надлишковим. У контексті безпеки цілком обгрунтованим постає умовивід дослідників про неадекватність і суттєве завищення суб'єктивного сприйняття характеру пов'язаних із відомостями загроз судами загальної юрисдикції, органами прокуратури й операторами в Україні [60, с.45; 83, с. 106; 92, с. 118].

Діючий механізм прокурорсько-судового контролю за доступом до розрахункових і службових даних не є позитивним моментом стосовно забезпечення безпеки. Зокрема, такий механізм призводить до ігнорування інтересів інших учасників суспільних відносин, а саме оперативних підрозділів. Не дивлячись на той факт, що останні виступають безпосередніми суб'єктами загроз, реалізація котрих обумовлена доступом до відомостей, глобалізація телекомунікаційної сфери

вимагає від них для результативного виконання свої зобов'язань перед людиною, суспільством і державою використання деталізацій і моніторингів як нового інформаційного джерела при документуванні злочинної діяльності, розкритті злочинів і розшуку злочинців тощо [50; 95, с. 119].

Слід також зазначити, що доступ оперативних підрозділів до відомостей шляхом їх безпосереднього витребування в операторів на підставі судового дозволу має й інші проблемні моменти. Зокрема, наявність у постанові суду абонентського номеру чи серійного номеру терміналу тощо призводить до неминучого розголошення інформації про здійснення оперативно-розшукових заходів або (та) слідчих дій стосовно конкретного споживача. Це, в свою чергу, може суттєво зашкодити документуванню та виявленню фактів противоправних діянь, а також інтересам кримінального судочинства. Актуальність указаної проблеми значно зростає, коли абонент є публічною особою, працівником оператора чи його близьким родичем тощо, та, цілком зрозуміло, що не зменшується при витребувані відомостей на підставі письмового запиту оперативного підрозділу [34; 101].

З іншого боку, ґрунтуючись на положеннях чинного законодавства, оператор майже без ризику застосування дієвих санкцій до себе завжди може відмовити у наданні деталізацій і моніторингів або ж суттєво затягти термін виконання відповідних вимог постанови суду чи письмового запиту оперативного підрозділу, посилаючись на сумнівні технічні причини. Загалом, працівниками операторів зв'язку на власний розсуд тлумачаться норми чинного законодавства України, самостійно приймаються рішення щодо обсягу і термінів надання інформації, яку запитують. Тому в Україні складаються умови для злочинів проти власності, предметом посягання у яких є термінал [73, с. 149; 76, с. 150; 82, с. 74].

Таким чином, аналіз правового аспекту забезпечення інформаційної безпеки людини в Україні як споживача телекомунікаційних послуг показав, що зараз українським законодавством не визначений інформаційно-правовий механізм, який дозволив би оперативним підрозділам якісно та законно взаємодіяти з операторами з приводу доступу до відомостей і одночасно передбачав би дієві інструменти забезпечення безпеки. В той час як результати аналітичної обробки

деталізацій і моніторингів у процесі здійснення оперативно-розшукової діяльності дозволяють ефективно викривати кримінальні злочини на території країни.

Приймаючи до уваги проблематику дослідження в межах роботи також був проведений аналіз статистичних даних стосовно злочинів, предметом посягання у яких стали термінали (мобільні телефони). Джерелом даних для аналізу послужили щорічні звіти Генеральної прокуратури України про зареєстровані кримінальні правопорушення та результати їх досудового розслідування [91]. Детальне вивчення відомості щодо злочинів в залежності від предмета посягання дозволило дослідити злочини проти власності, у яких предметом посягання є термінал (табл.2.1).

*Таблиця 2.1*

**Відомості про кількість злочинів проти власності, предметом злочинного посягання є термінал у 2010-2018 рр.**

| Роки | Усього злочинів проти власності | | |
|---|---|---|---|
| | загальна кількість | з них злочинів, у яких предмет посягання – термінал | |
| | | кількість | відсоток |
| 2010 | 306 963 | 68 070 | 22,2 |
| 2011 | 339 326 | 78 384 | 23,1 |
| 2012 | 336 604 | 82 468 | 24,5 |
| 2013 | 333 882 | 87 811 | 26,3 |
| 2014 | 310 559 | 83 540 | 26,9 |
| 2015 | 361 211 | 105 112 | 29,1 |
| 2016 | 404 453 | 122 954 | 30,4 |
| 2017 | 334 402 | 107 009 | 32,0 |
| 2018 | 303 850 | 100 574 | 33,1 |
| Джерело: звіти Генеральної прокуратури України за 2010-2018 рр. [91] | | | |

Відповідно до відомостей, наведених у табл.2.1, в Україні протягом 2010-2018 років залишається досить високим рівень злочинів проти власності (крадіжка, розбій, грабіж, вимагання та інші). Найбільш високий рівень був зафіксований у 2016 році (361 211 випадків). Не зважаючи на коливання загальної кількості

злочинів протягом аналізованого періоду постійно зростає кількість злочинів, у яких предметом посягання є термінал. На початку аналізованого періоду (у 2010 році) було зареєстровано 68 070 злочинів. Проте на у 2018 році було зареєстровано вже 100 574 таких злочинів, що на 32 504 злочини (або на 47,8%) більше у порівнянні з показниками за 2010 рік. Найвищий рівень злочинності спостерігався у 2016 році, коли було зареєстровано 122 954 злочини проти власності, у яких предмет посягання – термінал.

Слід також відзначити, що протягом 2010-2018 років стійкою залишається тенденція зростання відсотка злочинів, у яких предметом посягання є термінал у загальній структурі зареєстрованих злочинів проти власності. Зокрема, в 2010 році частка таких злочинів у загальній кількості зареєстрованих злочинів проти власності становила 22,2%. Протягом подальших 9 років частка таких злочинів зросла до 33,1%. Виходячи з результатів аналізу можна зробити висновок, що на сучасному етапі в Україні спостерігаються небувалі темпи розповсюдження злочинів, предметами посягань у яких є термінали (мобільні телефони).

Крім того, в межах дослідження доцільно розглянути структуру злочинів проти власності, предметом посягання у яких став термінал (рис.2.1). У відповідності до зображеної на рис.2.1 діаграми, у 2018 році найбільшу частину злочинів складають крадіжки (ст.185 КК України) – 55,3%. Значно поступаються крадіжкам наступні різновиди злочинів:

- грабіж (ст.186 КК України) – 29,1%;
- шахрайство (ст.190 КК України) – 10,3%;
- розбій (ст.187 КК України) – 4,1%;
- інші злочини (ст.188-189, ст.191-198 КК України) – 1,2% [91].

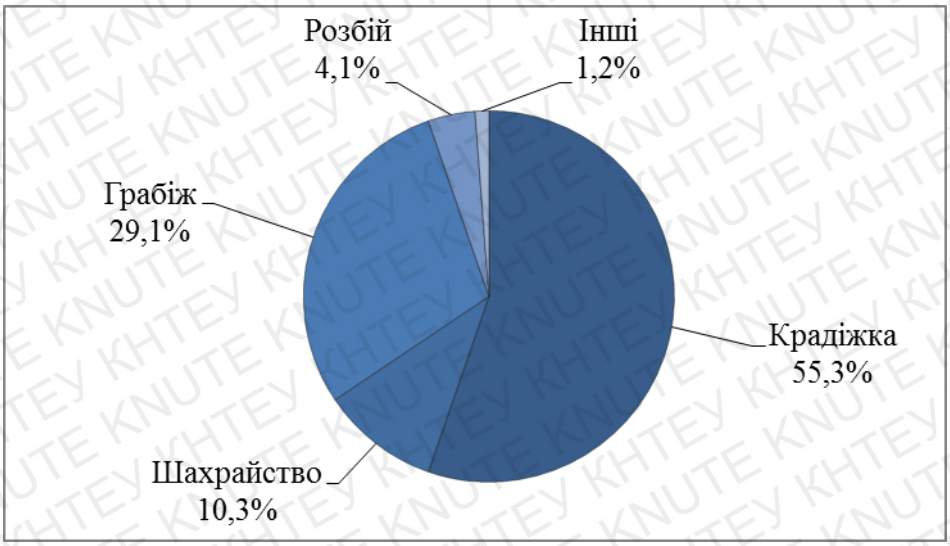


Рис.2.1. Різновиди злочинів, у яких предмет посягання є термінал у 2018 р. [91]

Наведена діаграма структури злочинів за статистичними даними 2018 року вказує на необхідність вживання термінових заходів, що направлені на зниження, перш за все, крадіжок мобільних телефонів. На наступному етапі аналізу необхідно розглянути динаміку кількості зареєстрованих та розкритих злочинів проти власності, предметом злочинного посягання є термінал (рис.2.2).

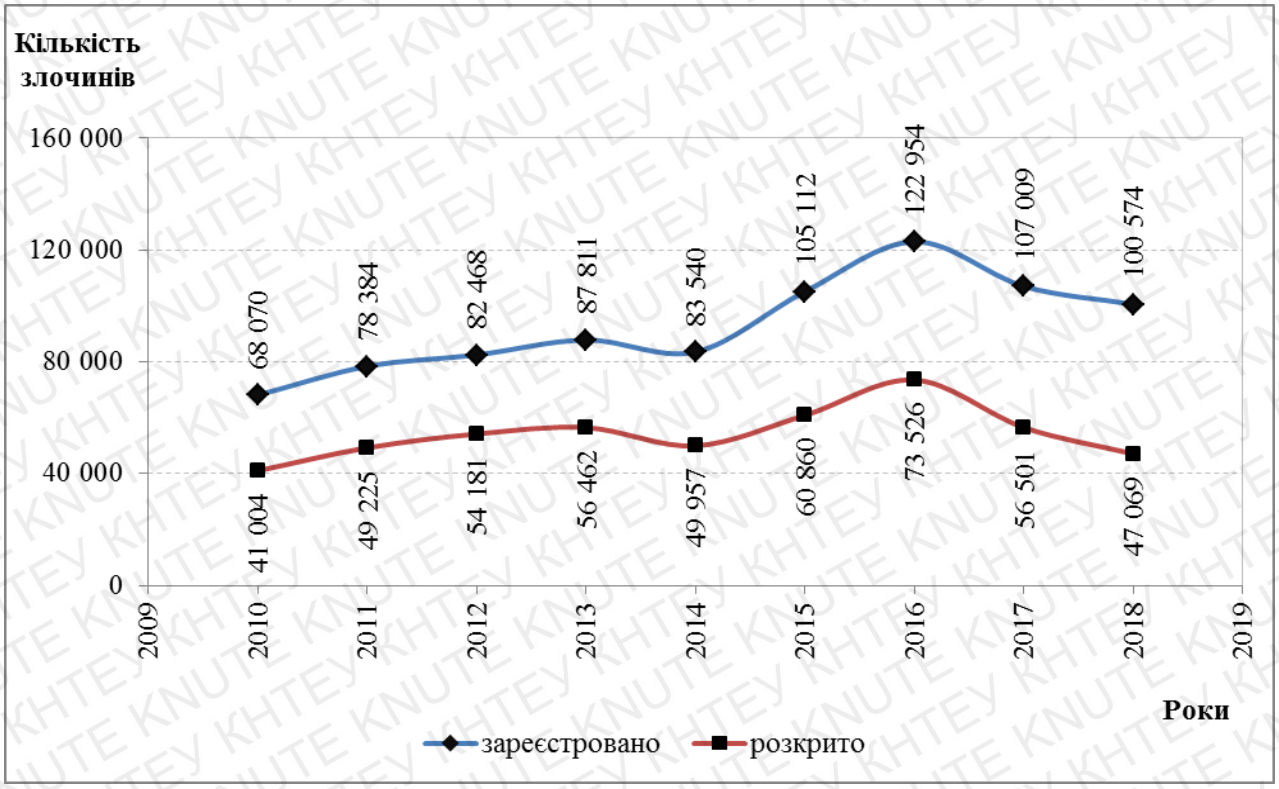


Рис.2.2. Динаміка кількості злочинів проти власності, предметом злочинного посягання є термінал (2010-2018 рр.) [91]

Як показує рис.2.2, кількість зареєстрованих злочинів проти власності, предметом злочинного посягання котрих є термінал збільшилась у 1,48 разів (100 574 : 68070) протягом 2010-2018 року. Одночасно з тим кількість злочинів, що були розкриті, збільшилась лише у 1,15 разів (47 069 : 41 004). Наведені дані свідчать про негативну тенденцію зниження частки розкритих злочинів у співвідношенні до кількості злочинів, що були зареєстровані. Динаміку розкритих злочинів проти власності, предметом злочинного посягання котрих є термінал, доцільно представити у вигляді графіку (рис.2.3).

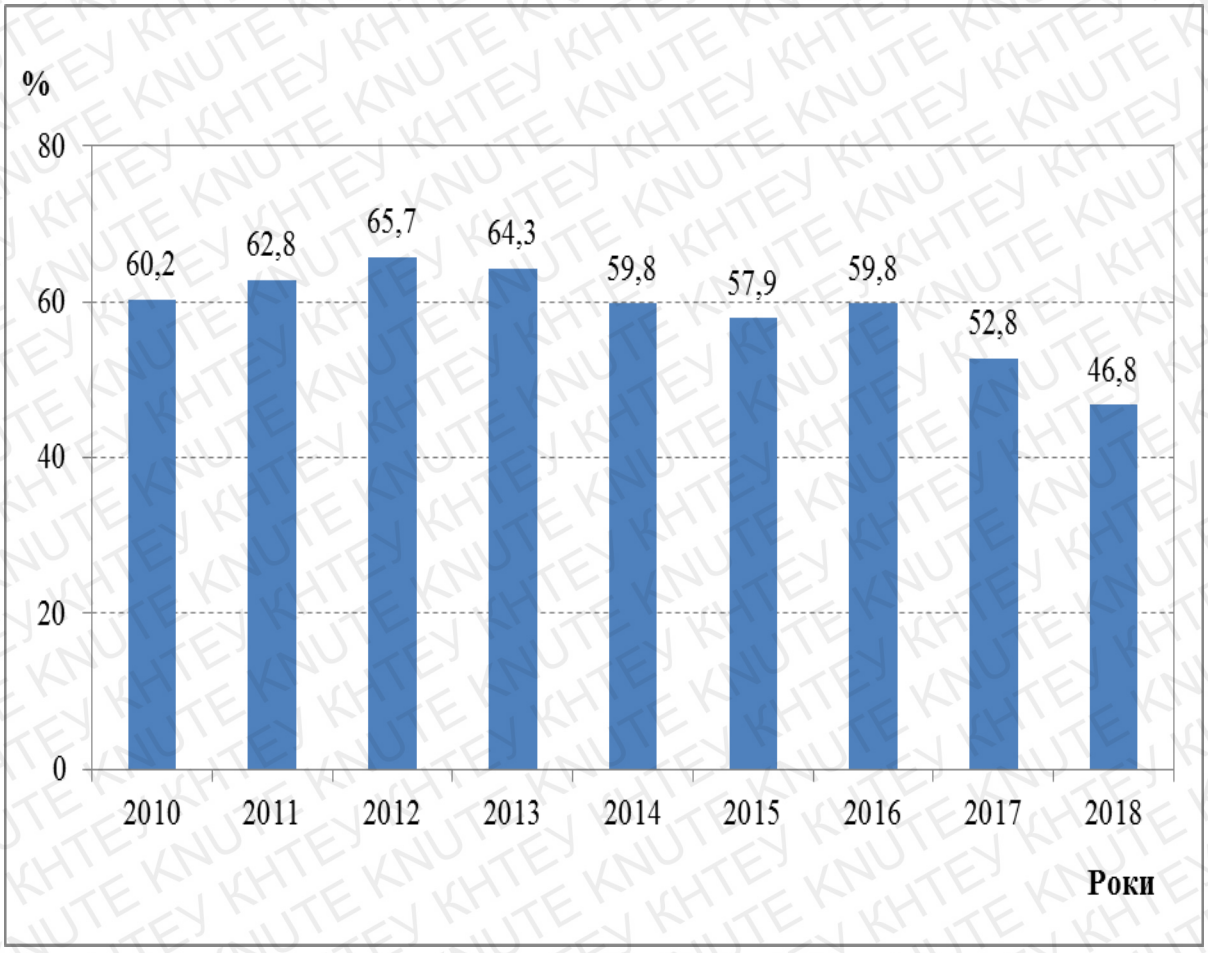


Рис.2.3. Відсоток розкритих злочинів проти власності, предметом злочинного посягання котрих є термінал (2010-2018 рр.) [91]

За даними Генеральної прокуратури України протягом 2010-2018 року спостерігається зниження відсотка розкритих злочинів проти власності, предметом злочинного посягання котрих є термінал, у порівнянні з зареєстрованими злочинами. Вагалі зменшення показника становило 13,4 відсоткових пунктів

(60,2% - 46,8%). Найбільший відсоток розкритих злочинів протягом аналізованого періоду був зафіксований у 2012 році та становив 65,7%. Інакше кажучи, приблизно третина злочинів залишилась нерозкритими у 2012 році. Постійне погіршення ситуації протягом 9 років призвело до того, що 53,2% (100% - 46,8%) зареєстрованих злочинів проти власності, предметом злочинного посягання котрих є термінал, залишаються нерозкритими. У середньому за сім років (2012-2018 рр.) частка розкритих злочинів по відношенню до зареєстрованих зменшується щорічно на 2,7 відсоткових пункта (65,7% - 46,8%) : 7). Виявлена тенденція зниження відсотку розкритих злочинів та постійне збільшення зареєстрованих злочинів проти власності, предметом злочинного посягання котрих є термінал, вказує на неефективність існуючого правового механізму регулювання у телекомунікаційній сфері, що ставить під загрозу безпеку кожної людини як споживача відповідних послуг.

Аналіз юридичних аспектів міжнародного та європейського права, а також закордонної практики доступу правоохоронних органів до відомостей дозволяє зробити висновок, що Україна не першою зіштовхнулася з питаннями забезпечення безпеки у сфері надання комунікаційних послуг. Більш того, нашою державою вже ратифіковано міжнародно-правові акти [2; 38], норми котрих у відповідності з позицією Європейського Парламенту та Ради Європейських Спільнот є юридичним базисом ефективного врегулювання суспільних відносин у даній сфері [8, абз. 20]. Однак, імплементація положень міжнародних документів у вітчизняне законодавство, як і реалізація інших заходів щодо гармонізації останнього з відповідними стандартами міжнародного та європейського права, зараз не може охарактеризуватися як однозначно продуктивною. Серед основних інформаційних небезпек для споживачів комунікаційних послуг залишаються загрози, обумовлені неправомірним доступом до відомостей. Однак, у даному аспекті чинне законодавство з питань забезпечення інформаційної безпеки людини в Україні як споживача телекомунікаційних послуг не відповідає динаміці змін, які є результатом розвитку інформаційного суспільства в світі. З цієї причини певні елементи останнього існують за межами правового поля та не регулюються

чинними нормативними актами. Крім того, до цього моменту відсутні нормативно-правові акти, затвердження та розробка яких передбачається чинним законодавством. Проекти актів, що були запропоновані, переважно є некоректними та недосконалими з точки зору їх відповідності чинному законодавству. У такій ситуації існуюча юридична неузгодженість та невизначеність провокує суб'єктів інформаційних відносин до неточного тлумачення законодавчих норм, є підґрунтям для зловживань у сфері надання телекомунікаційних послуг, обумовлені неправомірним доступом до відомостей.

Таким чином, проведений аналіз регулювання забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні та зарубіжного досвіду дозволяє сформувати перелік основоположних причин вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг, серед яких:

1) постійне зростання обсягів споживання телекомунікаційних послуг населенням у цілому, а також представниками кримінального середовища;

2) відсутність альтернативних розрахунковим та службовим даним джерел отримання оперативно важливої інформації про минулі телекомунікації таких категорій осіб, як свідки, підозрювані, безвісно відсутні та інші, під час здійснення правоохоронної діяльності;

3) службові зловживання щодо неправомірного доступу співробітників до відомостей у власних неслужбових потребах;

4) зростаючі темпи розповсюдження злочинних посягань на термінали та неефективність способів боротьби з ними, які б дозволили мінімізувати потреби вітчизняних оперативних підрозділів у відомостях з цього приводу;

5) неефективність діючого механізму прокурорсько-судового контролю за доступом оперативних підрозділів до розрахункових і службових даних.

## 2.2. Напрями вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг

Проведений у попередній частині дослідження нормативно-правових актів на національному та міжнародному рівні, а також аналіз стану забезпечення інформаційної безпеки людини в Україні вказують на необхідність вдосконалення правового забезпечення державного управління в сфері телекомунікаційних послуг. Зміни нормативно-правової бази сприятимуть вирішенню низки проблем, що існують на шляху гармонійного розвитку інформаційної сфери в межах країни. Зокрема, це дозволить визначити механізми державного регулювання відносин у сфері забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг.

Спираючись на проведений раніше аналіз, у межах даного дослідження доцільним буде зосередитися на питаннях, що пов’язані з інформаційно-правовим механізмом забезпечення доступу співробітників до розрахункових і службових даних під час оперативно-розшукової діяльності. В комунікаційній сфері дуже важливими є питання, пов’язані з безпекою людини як споживача телекомунікаційних послуг. Для вирішення цих питань необхідне врахування особливостей вітчизняної практики з протидії злочинності, а також положень відповідного міжнародного законодавства. Також для вирішення поставленого завдання необхідно враховувати сучасні тенденції, що спостерігаються у вітчизняній нормотворчі. Зокрема, у нашій державі протягом останніх років відбувається доволі активний процес, направлений на нормативне-правове врегулювання питань «перехоплення телекомунікацій», у межах якого й здійснюється доступ до відомостей з боку оперативних підрозділів. Взагалі можна погодитися із запропонованими в означеній сфері законопроектами на концептуальному рівні [50, 52, 53, 54, 55, 56, 57, 58, 59]. На наступному етапі дослідження необхідно конкретизувати напрями вдосконалення правового забезпечення в означеній сфері (рис.2.4).


Рис.2.4. Основні напрями вдосконалення правового забезпечення інформаційної безпеки у сфері телекомунікаційних послуг

Першим напрямом є регламентація терміну зберігання всіх категорій розрахункових та службових даних оперативними підрозділами та операторами. Крім того, нормативного врегулювання потребують вимоги, що визначають технологічні, організаційні та кваліфікаційні аспекти забезпечення захисту безпеки споживачів телекомунікаційних послуг. Вдосконалення перелічених аспектів дозволить конкретизувати юридичну відповідальність за порушення в сфері надання телекомунікаційних послуг. З огляду на міжнародний досвід зазначена складова проблеми безпеки частково вирішується, засновуючись на законодавчому врегулюванні суспільних відносин, що пов'язані із ліцензуванням у телекомунікаційній сфері та захистом персональних даних в процесі їх обробки. Слід відзначити, що у даному напрямі у вітчизняному законодавстві вже були зроблені позитивні кроки, що полягали у прийнятті нових законів та ратифікації міжнародних угод [2; 16; 28; 47; 48; 49].

Другим напрямом вдосконалення правового забезпечення безпеки у сфері споживання телекомунікаційних послуг є чітке визначення та закріплення первинної класифікації відомостей із урахуванням потенційно можливих та

існуючих систем, як це було зроблено в Європейському Союзі. Завдяки закріпленню на законодавчому рівні класифікації в теперішній час та в майбутньому буде цілком виключено ототожнення розрахункових та службових даних зі змістом повідомлення в процесі правозастосування.

Необхідно відзначити, в національній правотворчості вже були зроблені спроби розмежувати ці два поняття, зокрема, в законопроектах та підзаконних нормативно-правових актах, орієнтованих на врегулювання перехоплення телекомунікацій [50; 52; 53; 58; 59]. Однак упровадження правових інновації такого характеру доцільно починати з упорядкування українського законодавства в телекомунікаційній сфері, а саме положень Закону України «Про телекомунікації» [39]. Такий порядок змін в нормативному регулюванні означеної сфери дозволить уникнути правових колізій. Крім того, вирішення питання про розмежування розрахункових та службових даних зі змістом повідомлення важливе як в контексті оптимізації боротьби зі злочинністю, так й для охорони даних користувачів телекомунікаційних послуг від посягань інших суб'єктів загроз (а не тільки оперативних підрозділів).

До числа питань, що потребують першочергового вирішення на законодавчому рівні, також належить регулювання доступу оперативних підрозділів до службових і розрахункових даних. Означене питання визначає в межах даного дослідження третій напрям удосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг (див. рис.2.4). Відповідно до результатів аналізу, проведеного у попередніх частинах роботи, необхідність удосконалення механізму доступу оперативних підрозділів до службових і розрахункових даних обумовлена:

- неефективністю діючого в Україні варіанту нагляду та контролю за доступом співробітників до відомостей в аспекті забезпечення безпеки в сфері надання телекомунікаційних послуг;
- недосконалістю чинних правових норм, що визначають компетенцію оперативних підрозділів щодо витребування від інших учасників суспільних відносин потрібної інформації;

- дисертаційними дослідженнями та напрацюваннями стосовно відповідної зарубіжної правоохоронної практики;
- висновками міжнародних емпіричних досліджень конгресу ООН.

Спираючись на вказані вище підстави, представляється доцільним легітимізувати перехід від попереднього судового чи прокурорського до цілком відомчого санкціонування доступу до розрахункових та службових даних з боку оперативних підрозділів. Однак вказана новація у національному законодавстві повинна реалізовуватися за умови зміни інформаційно-правового механізму регулювання негласного доступу до необхідних відомостей. Перш за все, зміни в законодавстві повинні вдосконалити даний напрям оперативно-розшукової діяльності у телекомунікаційній сфері, а також виключити практичну доцільність безпосереднього витребування моніторингів та деталізацій у операторів. З іншого боку, необхідні дієві механізми забезпечення безпеки в сфері надання телекомунікаційних послуг. Зокрема, за допомогою автоматичного протоколювання дій кожного співробітника в означеній сфері, що за потреби надасть можливість перевіряти їх відповідність державними інституціями, окремими споживачами або громадськістю.

У даному випадку, говорячи про перехід до відомчого санкціонування доступу до розрахункових та службових даних, мова йде про перевлаштування вже розробленої раніше в Україні системи перехоплення для аналогічного загальноєвропейському «невибірковому збиранню даних трафіка» накопичення відомостей за межами систем операторів для розвідувальної та оперативно-розшукової діяльності. Одночасно з тим, реалізація даного нововведення повинна ґрунтуватися на науковому проробленні його нормативно-правового забезпечення в аспекті відповідності діючим стандартам Європейського суду з прав людини в питанні перехоплення даних без порушення Конвенції Ради Європи «Про захист прав людини та основоположних свобод» [3, ст. 8], а також іншим нормам міжнародного та національного законодавства [8; 50; 72; 79; 80; 102].

Для виконання означеного вище завдання необхідно відмітити недоліки організації отримання негласного доступу до відомостей співробітників з точки зору

забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг. Перш за все необхідно відмітити, що на сучасному етапі фактично існує монополія певних оперативних підрозділів на більшу частину елементів системи перехоплення[1] [41, ст. 3; 79; 80].

З огляду на проведений аналіз у попередніх частинах дослідження в розпорядженні всіх діючих «суб'єктів перехоплення» повинні перебувати лише «засоби управління системою перехоплення телекомунікації», зокрема, «віддалені термінали суб'єкта перехоплення»[2] [50, ст. 8]. Всі інші технічні засоби одночасно із функціями стосовно організаційно-технічного забезпечення їх експлуатації для забезпечення безпеки людини як споживача телекомунікаційних послуг доцільно перевести із компетенції оперативних підрозділів до прерогативи «спеціально уповноваженого координуючого органу з питань перехоплення телекомунікацій», який не виконує розвідувальну, контррозвідувальну чи оперативно-розшукову діяльність [52, ст. 8-10; 53, ст. 8].

Проте, слід відзначити, що пропозиція створення окремого органу, що займається питаннями перехоплення телекомунікацій, підштовхує до питання про доцільність цього кроку. Спираючись на результати вивчення чинного національного та закордонного законодавства, а також діючих механізмів державного управління в правоохоронній, телекомунікаційній, інформаційній та інших сферах , питання про доцільність може бути вирішеним за допомогою змін в правових нормах про статус, головні обов'язки, права та завдання діючої Державної служби спеціального зв'язку та захисту інформації України [22, ст. 2-4, ст. 16-18; 23, ст. 1; 32; 33] (далі – ДССЗЗІ). Цей державний орган був створений для забезпечення розвитку та функціонування державної системи урядового зв'язку та

---

[1] «До складу технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України відносяться: … мережний комплект (МК) для здійснення перехоплення телекомунікацій; … засоби управління системою перехоплення телекомунікації (сервери, станції, термінали та інші – ЗУСП); … засоби захищеної телекомунікаційної мережі спеціального призначення (ЗЗТМ); … програмне забезпечення (ПЗ) технічних засобів; … експлуатаційна та програмна документація технічних засобів; … комплект запасних інструментів та приладів (ЗІП)» [50, п. 4.1, п. 4.2].

[2] Віддалений термінал суб'єкта перехоплення – «обладнання, яке забезпечує приймання та обробку вмісту сеансів зв'язку, що передаються підрозділом перехоплення» [50, п. 4.1, п. 3.3].

інформаційних ресурсів в телекомунікаційних та інформаційних системах Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації.

Для регулювання доступу до службових і розрахункових даних представляється доцільним поширити наявні повноваження зазначеного вище державного органу для супроводження системи перехоплення. При цьому повний режим спостереження за об'єктами перехоплення [3] буде виконуватися через віддалені термінали суб'єктів перехоплення. У то же час механізм статистичного режиму спостереження за об'єктами перехоплення[4] буде принципового змінений.

В межах запропонованого розширення повноважень ДССЗЗІ за допомогою технічних засобів буде здійснювати невибіркове накопичення відомостей, що будуть надходити з систем операторів телекомунікаційних систем для подальшого надання моніторингів та деталізацій за потреби оперативних підрозділів (див. Додаток В). Втім, впровадження на практиці запропонованого нововведення вимагає розгорнутого наукового дослідження та подальших змін нормативно-правової бази, що стосується питань організації взаємодії між державними органами.

Крім того, аналіз чинного законодавства та діючого порядку системи перехоплення вказує на ще один суттєвий недолік правового аспекту забезпечення інформаційної безпеки. Результати дослідження дозволяють зробити висновок про відсутність технічних засобів, які будуть призначені для позавідомчого контролю або нагляду за реалізацією оперативно-розшукових заходів у національних телекомунікаційних мережах. Одночасно з тим в системі перехоплення важливо ввести засоби «гарантування законності». Адже функціонування останніх у комплексі із рекомендованими вище протоколюванням усіх дій співробітників і конкретизацією

---

[3] Об'єкт перехоплення являє собою «сеанси зв'язку абонента спостереження, інформація про його місцезнаходження та додаткова інформація про профіль послуг, що закріплені за терміналом абонента спостереження». абонент спостереження – це «особа, щодо якої здійснюється перехоплення телекомунікацій» [50, п. 3].

[4] « Для категорії повного режиму спостереження об'єкти перехоплення від МК до ЗУСП повинні передаватися у реальному часі… Для категорії статистичного спостереження від МК до ЗУСП передаються службові дані сеансів зв'язку у реальному часі" [50, п. 4.4]..

їх юридичної відповідальності в цій сфері не лише дієво сприятиме нейтралізації негативних наслідків для споживача від уже здійснених оперативними підрозділами зловживань, а й ефективно попереджатиме більшість потенційних загроз до їх реалізації.

На наступному етапі дослідження необхідно детально розглянути структурно-функціональні аспекти, пов'язані з міжвідомчим обігом відомостей. Однак, відповідно до вимог чинного національного законодавства охорони службової та державної таємниці стосовно нетаємного видання відомостей неможливо розглянути із достатнім ступенем деталізації всі аспекти порушеного питання. Тому в межах цього дослідження необхідно зосередитися на визначені концептуальних пропозицій з означеної проблематики.

Слід відзначити, що питання про вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг безпосередньо пов'язане з організацією відомчого обігу відомостей. У даному випадку представляється доцільним запропонувати дворівневу модель відомчого обігу відомостей (рис.2.5).

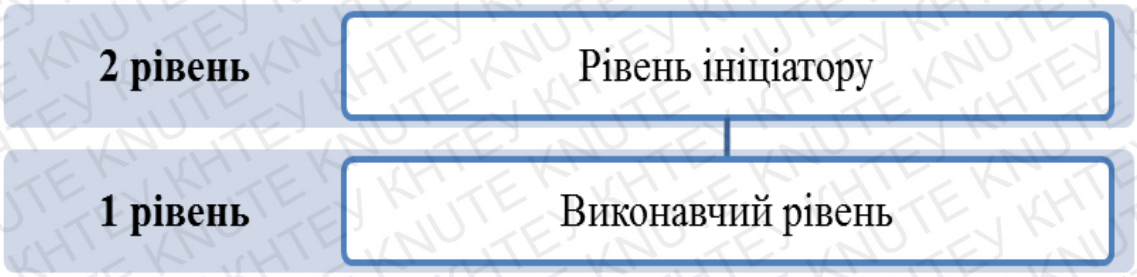


Рис. 2.5. Модель відомчого обігу відомостей

Відповідно до зображеної вище схеми на рис.2.5, виконавчий рівень здійснюватиметься безпосередньо оперативно-технічними підрозділами та відповідно із специфікою їх організації умовно може поділятися на регіональні та центральний підрівні. Саме на виконавчий рівень, що функціонально забезпечуватиметься спеціалізованою міжвідомчою захищеною інформаційно-телекомунікаційною системою, покладатиметься взаємодія з ДССЗЗІ щодо моніторингів та відбору деталізацій за запитами оперативних підрозділів, надання методичної та практичної допомоги їх співробітникам з обробки отриманих даних

тощо. Крім того, рівень ініціатору буде включає в себе оперативний підрозділ, робота якого націлена на електронний варіант отримання необхідних відомостей на електронних носіях інформації. Для рівня ініціатору необхідно укомплектовування та розробка спеціалізованого програмного забезпечення, що дозволить:

- виключити можливість несанкціонованої роздруківки, перегляду, спотворення моніторингів та деталізацій іншими програмними засобами;
- автоматизувати попередній аналіз вибірок тощо.

Таким чином, при проектуванні механізму міжвідомчого обігу розрахункових та службових даних необхідно враховувати наступні чинники:

1) доцільність інформатизації доступу до відомостей, що стосуються споживачів телекомунікаційних послуг;

2) відсутність реальної необхідності пристосування віддалених терміналах суб'єктів перехоплення» для статистичного спостереження за об'єктами перехоплення, оскільки до його реалізації пропонується застосувати ДССЗЗІ;

3) детальний аналіз нормативно-правових актів, що стосуються перехоплення телекомунікацій та технологічних аспектів оперативно-розшукової діяльності в мережах електрозв'язку, визначення однакових вимог до яких робить можливим проведення статистичного спостереження за об'єктами перехоплення;

4) нестача в оперативних підрозділах міського, міжрайонного та районного рівня співробітників із відповідними для ефективного використання моніторингів та деталізацій у боротьбі зі злочинністю досвідом і навичками.

**Висновки**

Серед головних проблем у сфері інформаційної безпеки України виняткове місце належить правовому регулюванню. Специфіка цієї проблеми виявляється в тому, що інформаційні відносини є складовою частиною всіх інших відносин – інтелектуальних, духовних, матеріальних тощо. З іншого боку, їх можна вважати суто інформаційними відносинами, окремо від об‘єктивного складу. На загальнодержавному та відомчому рівні обігу відомостей доцільно передбачити застосування адекватних технічних засобів для контролю за додержанням законів в процесі проведення оперативно-розшукової діяльності, що здійснюється органами прокуратури. Реалізація запропонованого механізму контролю допоможе забезпечити інформаційну безпеку людини в сфері надання комунікаційних послуг.

Службові та розрахункові дані виступають незамінним і, що важливо, найбільш раціональним в економічному плані джерелом оперативної інформації про телекомунікації таких категорій осіб, як підозрювані, обвинувачені, свідки, безвісно відсутні та інші. Заснований на масовому застосуванні службових і розрахункових даних найбільш апробований у вітчизняній оперативно-розшуковій практиці спосіб боротьби зі злочинними заволодіннями терміналами загалом не дає вагомих результатів та водночас сприяє реалізації загроз, пов’язаних із неправомірним доступом до деталізацій і моніторингів. Крім того, слід враховувати наявність негативних тенденцій в означеній сфері, зокрема, службові зловживання співробітників з приводу неправомірного доступу до відомостей як у власних неслужбових потребах, так і в службових інтересах протидії протиправним посяганням недостатнього ступеню суспільної небезпеки.

На основі статистичних узагальнень зроблено висновок про доцільність упровадження в Україні системи перехоплення для впровадження аналогічного загальноєвропейському «невибірковому збиранню даних трафіка» накопичення службових і розрахункових даних поза систем операторів для потреб оперативно-розшукової, розвідувальної та контррозвідувальної діяльності.

# ВИСНОВКИ

Здійснивши комплексне вивчення правових засад до забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг на підставі викладеного в кваліфікаційній роботі матеріалу можна зробити наступні висновки.

1. Процеси глобалізації сучасної цивілізаційної епохи здебільшого набувають вияву в інформаційній сфері, є заснованими на телекомунікаційному підґрунті та спричиняють неоднозначні для буття особи, суспільства й держави наслідки. З-поміж них як найактуальніші та злободенні для людини є перехоплення телекомунікацій, а також обмеження доступу споживачів до послуг.

2. Провідну роль у нейтралізації виявлених небезпек відіграє держава у процесі забезпечення інформаційної складової національної безпеки – інформаційної безпеки. Небезпеки та пов'язані з ними загрози вже доволі результативно опрацьовані та активно вивчатися з позицій різних наук, у їх числі й юридичних, а також знайшли своє закріплення у національному та міжнародному законодавстві. Однак чинне національне законодавство у низці аспектів відстає від динаміки змін, що виникають у процесі розвитку інформаційного суспільства. Тому частина елементів останнього існує за межами правового поля та не регулюється нормативними актами.

3. Аналіз позитивних здобутків європейських країн має важливе значення для вдосконалення діючої системи забезпечення інформаційної безпеки в Україні в аспекті правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг. Для подальшого розвитку Україна має орієнтуватися першочергово на стратегію розвитку та досвід країн-учасниць Європейського Союзу в інформаційній сфері.

4. Аргументовано доцільність визначення оперативних підрозділів як суб'єктів інформаційних правовідносин, що виникають під час витребування ними в інших суб'єктів – операторів – відомостей із метою подальшого їх використання у правоохоронній діяльності тощо. Доведено необхідність розгляду оперативних підрозділів у ролі не лише суб'єктів забезпечення безпеки, а й суб'єктів загроз.

5. Ґрунтуючись на теорії правовідносин, що розробляється фахівцями у галузі теорії держави і права, а також ураховуючи особливості функціонування сфери телекомунікацій України в умовах розвитку інформаційного суспільства, в роботі доведена необхідність виокремлення та дослідження в структурі інформаційних правовідносин нового предмета – відомостей, які водночас запропоновано розглядати як предмет безпеки. Доведено, що забезпечення безпеки в телекомунікаційній сфері суттєво залежить від якісного правового регулювання цих інформаційних правовідносин.

6. Оперативні підрозділи є суб'єктами інформаційних правовідносин, що виникають під час витребування ними в інших суб'єктів – операторів – відомостей із метою подальшого їх використання у правоохоронній діяльності тощо. В роботі доведена необхідність розгляду оперативних підрозділів у ролі не лише суб'єктів забезпечення безпеки, а й суб'єктів загроз.

7. Узагальнення практики використання відомостей операторами, споживачами й оперативними підрозділами дозволило стверджувати, що:

- вітчизняні оперативні підрозділи в умовах неухильного зростання кількості злочинних посягань на термінали не здатні дієво протидіяти розповсюдженню злочинності в телекомунікаційній сфері;
- концентрація зусиль і ресурсів оперативних підрозділів на розкритті незаконних заволодінь терміналами породжує сталу тенденцію загального зниження ефективності боротьби з майновою злочинністю.

**Пропозиції**

Для вдосконалення правового забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в роботі пропонується внести наступні зміни в чинне законодавство:

1. Одним із важливих напрямів вдосконалення правового забезпечення інформаційної безпеки у сфері споживання телекомунікаційних послуг є чітке визначення та закріплення первинної класифікації відомостей із урахуванням

потенційно можливих та існуючих систем, як це було зроблено в Європейському Союзі. Завдяки закріпленню на законодавчому рівні класифікації в теперішній час та в майбутньому буде цілком виключено ототожнення розрахункових та службових даних зі змістом повідомлення в процесі правозастосування.

2. Для оптимізації правового забезпечення також необхідно ввести законодавчу регламентацію термінів зберігання всіх категорій відомостей як операторами, так і оперативними підрозділами, визначення вимог правового, організаційного та іншого характеру щодо забезпечення їх захисту та конкретизації юридичної відповідальності за порушення в цій сфері.

3. З огляду на розроблені організаційно-правові пропозиції стосовно впорядкування обігу відомостей та вдосконалення забезпечення безпеки обґрунтовано раціональність і встановлено можливість переходу від попереднього прокурорського чи судового до суто відомчого санкціонування (як гласного, так і негласного) доступу оперативних підрозділів до службових і розрахункових даних.

4. Автоматичне протоколювання дій кожного співробітника стосовно доступу та використання відомостей з метою забезпечення можливості подальшої перевірки їх правомірності як відповідними державними інституціями та окремими споживачами. Це сприятиме нейтралізації негативних наслідків від зловживань оперативними підрозділами та ефективно убезпечуватиме від більшості потенційних загроз ще до їх реалізації.

5. В роботі була запропонована структурно-функціональну модель обігу службових і розрахункових даних на загальнодержавному та внутрішньовідомчому рівні. Закріплення даної моделі на правовому рівні дозволить вдосконалити вітчизняну систему перехоплення в інтересах забезпечення безпеки й оптимізації правоохоронної діяльності у сфері телекомунікацій.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція Міжнародного союзу електрозв’язку: підписано від імені України 22.12.1992 р. у м. Женеві; ратифіковано Законом України від 15.07.1994 р. №

116/94-ВР (редакція від 06.11.1998 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_100&p=1269285227358668.

2. Про захист осіб стосовно автоматизованої обробки даних особистого характеру : Конвенція Ради Європи від 28.01.1981 р. (вчинена в м. Страсбурзі): ратифіковано Законом України від 06.07.2010 р. № 2438-VI , (редакція від 06.07.2010 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_326&p=1284532981253799.

3. Про захист прав людини та основоположних свобод: Конвенція Ради Європи від 04.11.1950 р.: підписано від імені України 09.11.1995 р. в м. Страсбурзі ; ратифіковано Законом України від 17.07.1997 р. № 475/97-ВР (редакція від 02.10.2013 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_004&p=1284026246304765.

4. Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку: Директива Європейського Парламенту та Ради від 08.06.2000 р. № 2000/31/ЄС (Директива про електронну комерцію) [Електронний ресурс] // Переклад Центру порівняльного права при Міністерстві юстиції України; Веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_224&p=1274788268993388.

5. Про дозвіл електронних комунікаційних мереж та послуг : Директива Європейського Парламенту та Ради від 07.03.2002 р. № 2002/20/ЄС (Рамкова Директива) [Електронний ресурс] // Офіційний переклад Центру європейського та порівняльного права Міністерства юстиції України; Офіційне інтернет-представництво НКРЗ України. – Режим доступу: https://nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

6. Про доступ та з’єднання електронних комунікаційних мереж та пов’язаного оснащення: Директива Європейського Парламенту та Ради від 07.03.2002 р. № 2002/19/ЄС (Директива про доступ) [Електронний ресурс] // Офіційний переклад

Центру європейського та порівняльного права Міністерства юстиції України; Офіційне інтернет-представництво НКРЗ України. – Режим доступу: https://nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

7. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995 року [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_242.

8. Про збереження даних, що генеруються або обробляються у зв'язку з наданням загальнодоступних електронних послуг зв’язку або публічних мереж зв'язку та внесення змін до Директиви 2002/58/ЄС: Директива 2006/24 / ЄС Європейського Парламенту та Ради від 15.03.2006 р. [Електронний ресурс] // Official Journal. – 13.04.2006. – № L 105. – p. 54-63. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

9. Про обробку персональних даних та захист таємниці сектора електронних комунікацій (Директива про секретність та електронні комунікації): Директива Європейського Парламенту та Ради від 12.07.2002 р. № 2002/58/ЄС [Електронний ресурс] // Офіційний переклад Центру європейського та порівняльного права Міністерства юстиції України; Офіційне інтернет-представництво НКРЗ України. – Режим доступу: https://nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

10. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг: Резолюція Ради Європейського Союзу від 20.06.2001 р. № 9194/01, (ENFOPOL) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_234&p=1284026246304765.

11. Про спільні правові рамки для електронних комунікаційних мереж та послуг : Директива Європейського Парламенту та Ради від 07.03.2002 р. № 2002/21/ЄС (Рамкова Директива) [Електронний ресурс] // Офіційний переклад Центру європейського та порівняльного права Міністерства юстиції України; Офіційне інтернет-представництво НКРЗ України. – Режим доступу: https://nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

12. Про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг: Директива Європейського Парламенту та Ради від 07.03.2002 р. № 2002/22/ЄС (Директива про універсальні послуги) [Електронний ресурс] // Офіційний переклад Центру європейського та порівняльного права Міністерства юстиції України; Офіційне інтернет-представництво НКРЗ України. – Режим доступу : https://nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

13. Статут Міжнародного союзу електрозв'язку: підписано від імені України 22.12.1992 р. у м. Женеві; ратифіковано Законом України від 15.07.1994 р. № 116/94-ВР (редакція від 06.11.1998 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_099&p=1269285227358668.

14. Щодо конкуренції на ринках електронних комунікаційних мереж та послуг в цій сфері: Директива Комісії Європейських Спільнот від 16.09.2002 р. № 2002/77/ЄС (Текст дотичний ЄЕП) [Електронний ресурс] // Офіційний переклад Центру європейського та порівняльного права Міністерства юстиції України; Офіційне інтернет-представництво НКРЗ України. – Режим доступу: https://nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

15. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи від 28.01.2003 р. // Офіційний вісник України. – 2010. – № 56.

16. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних: Додатковий протокол від 08.11.2001 р. до Конвенції Ради Європи від 28.01.1981 р., (вчинений в м. Страсбурзі) : ратифіковано Законом України від 06.07.2010 р. № 2438-VI, (редакція від 06.07.2010 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_363&p=1284532981253799.

17. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР (редакція від 21.02.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради

України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

18. Господарський кодекс України: від 16.01.2003 р. № 436-IV (редакція від 21.10.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=436-15&p=1269953877570970.

19. Кримінальний кодекс України: від 05.04.2001 р. № 2341-III, (за станом на 18.10.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14&p=1282551389811708.

20. Цивільний кодекс України: від 16.01.2003 р. № 435-IV (редакція від 02.11.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15&p=1282551389811708.

21. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. № 2938-VI // Офіційний вісник України. – 2011. – № 10.

22. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV (редакція від 07.11.2018 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3475-15&p=1292253890017973.

23. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII (редакція від 05.08.2018 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/main/3855-12.

24. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI (редакція від 01.05.2015 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/main/2939-17.

25. Про друковані засоби масової інформації (пресу) в Україні: Закон від 16.11.1992 року № 2782-XII (редакція від 04.11.2018 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2782-xii.

26. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV (редакція від 07.11.2018 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-iv.

27. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.06.1994 р. № 80/94-ВР (редакція від 19.04.2014 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80.

28. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI (редакція від 30.01.2018 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/main/2297-17.

29. Про захист прав споживачів: Закон України від 12.05.1991 р. № 1023-XII (редакція від 16.07.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1023-12&p=1269284340622702.

30. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (редакція від 16.07.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-xii.

31. Про національну безпеку України: Закон України від 21.06.2018 р. №2469-VIII (редакція від 21.06.2018 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-viii.

32. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР (редакція від 01.08.2016 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

33. Про Національну систему конфіденційного зв`язку: Закон України від 10.01.2002 р. № 2919-III (редакція від 19.04.2014 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2919-14&p=1269285227358668.

34. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII (редакція від 22.05.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2135-12&p=1282551389811708

35. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 р. № 3341-XII (редакція від 05.01.2017 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3341-12&p=1270639103695902.

36. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V (редакція від 09.10.2007 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/537-v.

37. Про радіочастотний ресурс України : Закон України від 01.06.2000 р. № 1770-III (редакція від 17.10.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1770-14&p=1274788268993388.

38. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824- IV (редакція від 14.10.2010 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15.

39. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV (редакція від 16.07.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1280-iv.

40. Про Доктрину інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс] // Офіційне інтернет-представництво Президента України. – Режим доступу: https://www.president.gov.ua/documents/472017-21374.

41. Про додержання прав людини під час проведення оперативно-технічних заходів: Указ Президента України від 07.11.2005 р. № 1556/2005 [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1556%2F2005&p=1292253890017973.

42. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: затверджено Постановою Кабінету Міністрів України від 29.03.2006 р. № 373 (редакція від 13.10.2011 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=373-2006-%EF&p=1260376274430794.

43. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 08.10.1997 р. № 1126 (редакція від 13.10.2011 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF.

44. Про затвердження Правил надання та отримання телекомунікаційних послуг: Постанова Кабінету міністрів України від 11.04.2012 р. №295 (редакція від 06.07.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: https://zakon4.rada.gov.ua/laws/show/295-2012-%D0%BF.

45. Концепція розвитку телекомунікацій в Україні: схвалено розпорядженням Кабінету Міністрів України від 07.06.2006 р. № 316-р. (редакція від 27.12.2008 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=316-2006-%F0&p=1247747516744013.

46. План заходів, спрямованих на виконання обов’язків та зобов’язань України, що випливають з її членства в Раді Європи : затверджено розпорядженням Кабінету Міністрів України від 23.07.2008 р. № 1002-р , (редакція від 08.02.2017 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1002-2008-%F0&p=1284026246304765.

47. Ліцензійні умови здійснення діяльності у сфері телекомунікацій з надання послуг рухомого (мобільного) телефонного зв’язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в

користування каналів електрозв’язку: затверджено рішенням Національної комісії з питань регулювання зв’язку України від 26.01.2006 р. № 179 (редакція від 22.09.2017 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0145-06&p=1270639103695902

48. Ліцензійні умови здійснення діяльності у сфері телекомунікацій з надання послуг фіксованого телефонного зв’язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв’язку: місцевого, міжміського, міжнародного : затверджено рішенням Національної комісії з питань регулювання зв’язку України від 10.12.2009 р. № 1789 , (редакція від 01.11.2016 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0019-10&p=1270639103695902

49. Ліцензійні умови користування радіочастотним ресурсом України : затверджено рішенням Національної комісії з питань регулювання зв’язку України від 19.08.2005 р. № 53 , (редакція від 01.03.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z1237-05&p=1270639103695902.

50. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги: затверджено наказом Служби безпеки України та Міністерства транспорту та зв’язку України від 31.07.2008 р. № 645/962 [Електронний ресурс] / Ліга закон. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/FIN39887.html.

51. Звід відомостей, що становлять державну таємницю : затверджено наказом Служби безпеки України від 12.08.2005 р. № 440 (редакція від 17.09.2019 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0902-05&p=1287562074797785.

52. Про перехоплення телекомунікацій: проект Закону України № 4042-1 від 07.09.2004 р. [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=17622.

53. Про перехоплення телекомунікацій : проект Закону України № 4042-2 від 21.03.2005 р. [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=24030.

54. Висновок на проект Закону України «Про внесення змін до деяких Законів України (щодо недопущення незаконного обмеження конституційних прав людини під час досудового слідства, оперативно-розшукової та контррозвідувальної діяльності)» , (реєстр. № 4106 від 23.02.2009 р.) [Електронний ресурс] / Веб-сайт Верховної Ради України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=34561

55. Висновок на проект Закону України «Про внесення змін до деяких Законів України (щодо вдосконалення механізму захисту конституційних прав громадян при провадженні оперативно-розшукової та контррозвідувальної діяльності)», (реєстр. № 4663 від 12.06.2009 р.) [Електронний ресурс] / Веб-сайт Верховної Ради України. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=36693&pf35401=15870

56. Висновок на проект Закону України «Про внесення змін до статті 39 Закону України «Про телекомунікації» (про основи національної безпеки в сфері телекомунікацій)», (реєстр. № 7023 від 29.07.2010 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=38362&pf35401=179013.

57. Висновок на проект Закону України «Про внесення змін до частини четвертої статті 39 Закону України «Про телекомунікації» (щодо встановлення на телекомунікаційних мережах технічних засобів для перехоплення комунікацій і оплати цього уповноваженими органами)», (реєстр. № 7023-1 від 02.09.2010 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=38444.

58. Висновок на проект Закону України «Про перехоплення телекомунікацій», (реєстр. № 4042-1 від 02.06.2005 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=17622

59. Висновок на проект Закону України «Про перехоплення телекомунікацій" , (реєстр. № 4042-2 від 21.03.2005 р.) [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=24030.

60. Арістова І.В. Інформаційна безпека людини як споживача телекомунікаційних послуг : монографія / І.В. Арістова, Д.В. Сулацький. – К. : Право України, 2013. – 184 с.

61. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: дис. … доктора юрид. наук : спец. 12.00.07 / Ірина Василівна Арістова. – Харків: НУВС, 2014. – 476 с.

62. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України // Вісник Національної академії державного управління при Президентові України. – 2014. – № 3. – С. 60-65.

63. Богуцький О. А. Договори про надання телекомунікаційних послуг : автореф. дис. … канд. юрид. наук: 12.00.03 / Олександр Андрійович Богуцький. – К.: НДІ приватного права і підприємництва АПрН України, 2010. – 20 с.

64. Бондар І.Р. Інформаційна безпека як основа національної безпеки / І.Р. Бондар // Mechanism of Economic Regulation. – 2014. – № 1. – С. 68-75.

65. Волеводз А. Г. Протидія комп'ютерним злочинам: правові основи міжнародного співробітництва / А. Г. Волеводз. – М : Юрлитинформ, 2016. – 496 с.

66. Голотенко О. Відстежувати чи ні IP-адреси інтернет-піратів? Розбіжності судів США і Європи [Електронний ресурс] / О. Голотенко // Право. – Режим доступу: https://pravo.ru/interpravo/news/view/38474/

67. Горбулін В.П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України: монографія / В.П. Горбулін, А.Б. Качинський. – К.: Євроатлантикінформ, 2014. – 592 с.

68. Грабар Н.С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства [Електронний ресурс] / Н.С. Грабар // Електронний журнал «Державне управління: удосконалення та розвиток». – 2019. – №7. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=1461.

69. Гурковський В.І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства / В.І. Гурковський // Правова інформатика. – 2016. – №2(26). – С. 72-77.

70. Доповідна записка стосовно незаконних заволодінь мобільними телефонами : лист МВС України від 06.08.2003 р. № 8284/Гн // Справа УКР УМВС України в Донецькій області № 4/2. – 2004. – Т. 1. – 194 с. – С. 12-15

71. Жарков Я.М., Дзюба М.Т., Замаруєва І.В. Інформаційна безпека особистості, суспільства, держави: підручник / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва. – К.: Київський університет, 2016. – 274 с.

72. Законодавство щодо затримування даних: порушення прав, гарантованих Європейською конвенцією з прав людини : доповідь для «Privacy International» [Електронний ресурс] / пер. З англ. Р. Тополевського // Права людини: он-лайн-бібліотека Харківської правозахисної групи. – Режим доступу: http://library.khpg.org/index.php?id=1105737512.

73. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія / О.О. Золотар. – К.: Видавничий дім «АртЕк», 2018. – 446 с.

74. Калюжний Р.А. Питання концепції реформування інформаційного законодавства України / Р.А. Калюжний // Правове, нормативне та метрологічне забезпечення системи інформації в Україні: Тематичний збірник праць учасників Другої науково-технічної конференції. – К., 2015. – С.17-21.

75. Конєва О.І. Проблеми захисту інформації / О.І. Конєва // Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р.; Маріупольський державний університет;

Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – С.53-55.

76. Корж І.Ф. Внутрішні фактори загроз і викликів інформаційній безпеці України / І.Ф. Корж // Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук.-практ. конф. 06.10.2016 р. Упоряд.: В.М. Фурашев. – Київ: Політехніка, 2016. – С. 148-151.

77. Ксенофотова А.Е. Нормативно-правове забезпечення у інформаційній сфері України // Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р.; Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – С.57-59.

78. Ліпкан В.А., Логінов О.В., Харченко Л.С. Інформаційна безпека України: глосарій / В.А. Ліпкан, О.В. Логінов, Л.С. Харченко. – К.: Текст, 2004. – 136 с.

79. Лист Служби безпеки України від 21.10.2004 р. № 13/2/1-4186 [Електронний ресурс] // Сайт Генеральної прокуратури України. – Режим доступу: https://www.gp.gov.ua.

80. Лист УОТЗ при УМВС України в Донецькій області від 27.08.2005 р. № 40/2763 [Електронний ресурс] // Сайт Генеральної прокуратури України. – Режим доступу: https://www.gp.gov.ua.

81. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці / А.І. Марущак // Правова інформатика. – 2015. – №3(27). – С. 17-21.

82. Меживой В.П. Взаємодія підрозділів кримінальної міліції з операторами мобільного зв’язку з метою встановлення місцезнаходження викрадених мобільних терміналів / В. П. Меживой // Взаємодія правоохоронних органів з провайдерами та операторами зв’язку в боротьбі з комп’ютерними злочинами : Матеріали регіонального наук.-практ. Семінару. – Донецьк : ДЮІ ЛДУВС, 2014. – С. 73-75.

83. Мороз Н.С. Проблеми правового регулювання інформаційних відносин / Н.С. Мороз // ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. – Львів: Львівська політехніка, 2016. – С.105-107.

84. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

85. Нечипорук Ю.М. Інформаційна сфера як об’єкт адміністративної науки / Ю.М. Нечипорук // Порівняльно-аналітичне право. – 2017. – №2. – С. 128-131.

86. Злочини, пов'язані з використанням комп'ютерної мережі. Довідковий документ для семінару-практикуму по використанню комп'ютерної мережі: A/CONF.187/10 [Електронний ресурс] // Десятий Конгрес ООН з попередження злочинності та поводження з правопорушниками (м. Відень, 10-17.04.2000 р.); Веб-сайт ООН. – Режим доступу: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-RU.pdf.

87. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах / М.М. Присяжнюк // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. – 2016. – Вип. 30. С. – 42-46.

88. Про закріплення співробітників відділу боротьби з організованими групами та злочинними організаціями загальнокримінальної спрямованості УБОЗ ГУМВС України в Донецькій області за лініями робіт : розпорядження УБОЗ ГУМВС України в Донецькій області від 23.04.2009 р. № 87 [Електронний ресурс] // Сайт Генеральної прокуратури України. – Режим доступу: https://www.gp.gov.ua.

89. Прослуховування телефонів в міжнародному праві і законодавстві одинадцяти європейських країн [Електронний ресурс] / Е. Захаров // Інформаційний портал Харківської правозахисної групи. – Режим доступу: http://www.khpg.org.ua/index.php?id=1084719187.

90. Про створення оперативно-пошукового відділення щодо забезпечення розкриття тяжких злочинів, які здійснюються з використанням технічних засобів мобільного стільникового зв’язку: розпорядження УКР УМВС України в Донецькій області від 17.03.2004 р. № 1/993/4 [Електронний ресурс] // Сайт Генеральної прокуратури України. – Режим доступу: https://www.gp.gov.ua.

91. Стан та структура злочинності в Україні (2010-2018 рр.): статистика [Електронний ресурс] // Сайт Генеральної прокуратури України. – Режим доступу: https://www.gp.gov.ua/ua/statinfo.html.

92. Сулацький Д.В. Організаційно-правові засади забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг: дис. ... канд. юридичних наук: 12.00.07 / Д.В. Сулацький. – Херсон : Міжнар. ун-т бізнесу та права, 2011. – 290 с.

93. Сулацький Д. В. Організаційно-правові засади визначення відомостей щодо наданих телекомунікаційних послуг / Д. В. Сулацький // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку у боротьбі з комп'ютерними злочинами : Матеріали наук.-практ. семінару – Донецьк : ДЮІ ЛДУВС, 2009. – 152 с. – С. 117-129.

94. Сулацький Д. В. Проблеми використання можливостей інформаційно-телекомунікаційних технологій у розшуку злочинців / Д. В. Сулацький // Розшукова робота ОВС: проблеми та шляхи їх вирішення : Матеріали міжвуз. наук.-практ. Семінару; м. Донецьк, 28.03.2008 р. – Донецьк: ДЮІ ЛДУВС, 2008. – 220 с. – С. 69-74.

95. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … доктора юридичних наук: 12.00.07 / Тарас Юрійович Ткачук. – Ужгород: Ужгородський національний університет, 2019. – 487 с.

96. Ткачук Т.Ю. Забезпечення інформаційної безпеки: досвід окремих країн Європи / Т.Ю. Ткачук // Інформація і право. – 2017. – №4. – С. 62-72.

97. Фурашев В.М. Законодавче забезпечення інформаційної безпеки України / В.М. Фурашев // Інформація і право. – 2018. – №1. – С. 59-67.

98. Хаба Р.С. Деструктивні інформаційні впливи в сучасних умовах / Р.С. Хаба // Інформаційна безпека людини, суспільства, держави. – 2017. – № 1(21). – С. 216-224.

99. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України / В.Т. Шатун // Наукові праці Чорноморського державного університету імені Петра Могили. – 2016. – Т. 267. – Вип. 255. – С. 174-180.

100. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека [Електронний ресурс] / В.І. Шульга // Електронний журнал «Ефективна економіка». – 2015. – № 4. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5514.

101. Щодо можливості інформування суб'єкта господарювання про номер оперативно-розшукової справи : лист Міністерства юстиції України від 15.07.2009 р. № Н-16798 [Електронний ресурс] // Веб-сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=v6798323-09&p=1282551389811708.

102. Щодо проекту Директиви Європейського Парламенту і Ради «Про затримання даних, що обробляються у зв'язку з наданням публічних електронних комунікаційних послуг, і внесення змін до Директиви 2002/58/ЄС»: висновки Європейського наглядача із захисту даних від 26.09.2005 р. // П равова інформатика. – 2008. – № 3 (19). – С. 81-91.

103. Austrian Security Strategy (Vienna, July 2013) [Електронний ресурс] – Режим доступу:
http://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf.

104. CERT-Fi [Електронний ресурс] // TraFiCom. – Режим доступу: http://www.cert.fi/en/index.html.

105. Common Criteria for Information Technology Security Evaluation (1996) [Електронний ресурс]. – Режим доступу: https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf.

106. Communication from the Commission : Towards a general policy on the fight against cybercrime. COM (2007) [Електронний ресурс]. – Режим доступу: http://eurlex.europa.eu/LexUriServ/site/en/com/ 2007/com2007_0267en01.pdf.

107. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing

preparedness, security and resilience. COM (2009)149 [Електронний ресурс]. – Режим доступу: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqhne787z0.

108. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298 [Електронний ресурс] // European Commission. – Режим доступу: https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf.

109. Document C-V(2002)49: Security within the North Atlantic Treaty Organization (NATO) [Електронний ресурс]. – Режим доступу: http://www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf.

110. Dunn E.J. NATO clause V could deter cyber attack, says defence minister [Електронний ресурс] / John E. Dunn // NetworkWorld. – Режим доступу: https://www.networkworld.com/article/2194246/nato-clause-v-could-deter-cyberattack--says-defence-minister.html.

111. Federal Act on Data Protection (FADP) of 19 June 1992 [Електронний ресурс] // The federal Council. The portal of the Swiss government. – Режим доступу: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html.

112. General Data Protection Regulation [Електронний ресурс] // InterSoft Consulting. – Режим доступу: https://gdpr-info.eu/.

113. Information Technology Security Evaluation Criteria (1991) [Електронний ресурс]. – Режим доступу: https://pdfs.semanticscholar.org/facd/bd4b410670431e3f0ec2cf3dabcc7ef55545.pdf?_ga=2.231818655.1421295646.1571813280-1393289779.1571813280.

114. National Cyber Security Strategy (2015-2017) [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf.

115. NATO Bucharest Summit Declaration, 3 April 2008 [Електронний ресурс] // North Atlantic Treaty Organization. Official texts (Chronological). – Режим доступу: http://www.nato.int/docu/pr/2008/p08-049e.html.

116. NATO Lisbon Summit Declaration, 20 Nowember 2010 : [Електронний ресурс] // North Atlantic Treaty Organization. – Режим доступу: http://www.nato.int/docu/pr/2010/p10-049e.html.

117. NATO Warsaw Summit Communiqué, 9 July 2016 [Електронний ресурс] // North Atlantic Treaty Organization. – Режим доступу: http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

118. North Atlantic Treaty Organization. Active Engagement. Modern Defence Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation [Електронний ресурс] // North Atlantic Treaty Organization. – Режим доступу: https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

# ДОДАТКИ

**Додаток А**

Сфери національної безпеки [71, с. 15]

**Додаток Б**

Практика доступу оперативних підрозділів до відомостей щодо наданих телекомунікаційних послуг


Рис. Б.1.
Практика до 2005 року


Рис. Б.2.
Практика у 2005-2008 роках


Рис. Б.3.Практика з 2008 року

**Додаток В**

Запропонована модель доступу до відомостей щодо наданих телекомунікаційних послуг