легалізацією (відмиванням) майна, одержаного злочинним шляхом.

Відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» (в редакції від 04.07.2020 року), інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1]. Водночас, телекомунікаційна система – це сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [1].

Нами досліджено судову практику в Україні за останні десять років, а також аналітичні звіти деяких правоохоронних органів іноземних країн, які займаються боротьбою зі злочинністю, пов'язаною із легалізацією майна, отриманого злочинним шляхом, та виокремлено основні види інформаційно-телекомунікаційних систем та технологій, які використовуються з метою вчинення даного виду злочину, серед яких інформаційно-телекомунікаційні технології (ІКТ) та інформаційно-телекомунікаційні системи (ІКС).

Для загального розуміння проблематики розслідування кримінальних правопорушень, пов'язаних із легалізацією (відмиванням) майна, одержаного злочинним шляхом, із використанням інформаційно-телекомунікаційних систем та технологій, необхідно зазначити, що злочинці при вчиненні таких протиправних діянь використовують такі інформаційно-телекомунікаційні технології (ІКТ):

- комп'ютерна техніка, мобільні пристрої та встановлене на них програмне забезпечення, що в сукупності становить електронно-обчислювальні машини (ЕОМ) [2];
- телекомунікаційні системи (бездротовий телефонний або інтернет зв'язок, застосування медіа трансляцій, мессенджерів та додатків або програмного забезпечення задля усіх видів обробки відео та аудіо файлів);
- інтернет-банкінг (система дистанційного обслуговування клієнтів банку або інших фінансових інструментів);
- цифрові платіжні системи (наприклад, Google Pay, Pay Pall), онлайн гаманці (наприклад, Epay, WebMoney), електронні-валютні біржі та аукціони (наприклад, Binance);
- інші інструменти ІКТ та ІКС тощо.

Отже, «світова фінансова революція» та розвиток «передових цифрових технологій», проникнення мережі Інтернет на ЕОМ в усі сфери нашого життя, є результатом появи різноманітних способів легалізації (відмивання) майна, одержаного злочинних шляхом за допомогою різних видів інформаційно-телекомунікаційних систем та технологій. У зв'язку із чим постає питання в чіткому законодавчо закріпленому розмежуванні понять, які є суміжними з такою областю знань, як інформаційні технології (ІТ), що, в свою чергу, потребує більш досконалої розробки диспозицій статей особливої частини КК України з метою неможливості уникнення відповідальності за вчинені злочини.

---

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР (в редакції від 04.07.2020 року): URL: https://zakon.rada.gov.ua/laws/main/index (дата звернення 12.01.2023 р.).
2. Верховний Суд України – офіційний веб-сайт, URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02 (дата звернення 19.01.2023 р.).

УДК 004.77+355.02
DOI: 10.31733/17-03-2023-546-549

Сергій РОМАШКО
аспірант кафедри
економіки та соціально-трудових відносин
Університету митної справи та фінансів

КОНКУРЕНЦІЯ НА РИНКУ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ЯК ФАКТОР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВІЙСЬКОВИЙ ЧАС

Під час надзвичайних ситуацій та воєнного часу інформаційна безпека стає ще більш важливою, ніж у мирний час, адже це може бути питанням життя чи смерті. Своєчасне та точне поширення інформації може допомогти запобігти та пом'якшити наслідки катастроф,

а також координувати дії військових. Однак досягнення інформаційної безпеки може бути складним завданням, оскільки існують різні типи загроз, зокрема кібератаки, фізичне пошкодження інфраструктури та навмисна дезінформація.

Телекомунікаційні послуги відіграють вирішальну роль у забезпеченні інформаційної безпеки, надаючи необхідну інфраструктуру та засоби зв'язку. Надійна та міцна телекомунікаційна інфраструктура необхідна для своєчасного та точного зв'язку, який є життєво важливим під час надзвичайних ситуацій та воєнного часу.

Висока конкуренція на ринку телекомунікаційних послуг також має значення для забезпечення інформаційної безпеки. Конкуренція стимулює інновації та заохочує телекомунікаційні компанії інвестувати в покращення своєї інфраструктури, роблячи її більш надійною та міцною, а присутність на ринку більшої кількості операторів призводить до надлишкової кількості мереж, що дуже важливо у воєнний час, коли ризики пошкоджень мереж занадто високий.

Концепція інформаційної безпеки є складною і багатоаспектною [1]. Згідно з визначенням, запропонованим Міжнародною організацією зі стандартизації (ISO), інформаційна безпека - це стан забезпечення конфіденційності, цілісності та доступності інформації.

Телекомунікаційні послуги займають центральне місце в суспільному житті, забезпечуючи швидкий і зручний доступ до інформації, а також забезпечуючи зв'язок між різними регіонами світу. У сучасному світі, де інформація є ключовим ресурсом, телекомунікаційні послуги стають все важливішими в області національної безпеки та захисту інтересів країни.

Однією з найважливіших функцій телекомунікаційних послуг є забезпечення інформаційної безпеки. У цьому контексті, телекомунікаційні послуги включають в себе захист інформації, яка передається по мережі, а також захист від хакерських атак і вірусів. У сучасному світі, коли інформація є цінним активом, телекомунікаційні послуги відіграють важливу роль в захисті інформації від небажаних осіб.

Також, телекомунікаційні послуги є надзвичайно важливими в часи кризи та воєнного стану. У разі війни, телекомунікаційні послуги забезпечують зв'язок між різними частинами армії, а також надають зв'язок для цивільного населення, яке може перебувати в областях, що були зайняті ворогом. Також, телекомунікаційні послуги забезпечують зв'язок з іншими країнами для отримання допомоги та підтримки.

Під час надзвичайних ситуацій та воєнних дій на передній план стає проблема збереження сталих телекомунікацій і, як похідна – проблема збереження цілісності мереж та з'єднань, оскільки без збереження цілісності мереж здійснення сеансів передачі даних, голосу, відео є неможливими.

Тому одним із шляхів вирішення питань сталості телекомунікацій є залучення на ринок більшої кількості гравців. Інвестиційний потенціал галузі зичить цьому.

Телекомунікаційна галузь характеризується гострою конкуренцією, коли численні провайдери змагаються за частку ринку. Є кілька факторів, які сприяють такому високому рівню конкуренції:

А) Технологічний прогрес – телекомунікаційна галузь є залежною від розвитку технологій, що призвів до зростання конкуренції. Нові технології, такі, як 5G і волоконно-оптичні мережі, полегшили новим гравцям вихід на ринок.

Б) Дерегуляція телекомунікаційної галузі – вона призвела до посилення конкуренції, оскільки бар'єри входу були знижені, що дозволило новим гравцям вийти на ринок і конкурувати з відомими провайдерами.

В) Конвергенція послуг – призвела до зростання конкуренції, оскільки постачальники телекомунікацій пропонують ширший спектр послуг, розширений за рахунок появи, поряд з послугами передачі голосу та даних, телебачення та потокових послуг, хмарних обчислень та інших додаткових послуг.

Г) Глобалізація телекомунікаційної галузі – цей фактор посилив конкуренцію, оскільки провайдери з різних країн змагаються за частку ринку. З розвитком Інтернету та збільшенням доступності транскордонних послуг провайдери телекомунікацій більше не обмежуються своїми внутрішніми ринками.

Д) Попит клієнтів на високоякісні послуги за конкурентоспроможними цінами – він також сприяв посиленню конкуренції в телекомунікаційній галузі. Оскільки клієнти стають все більш обізнаними в техніці та вимагають більше від своїх провайдерів, телекомунікаційні компанії змушені впроваджувати інновації та надавати кращі послуги,

щоб утримати своїх клієнтів.

Підсумовуючи сказане, можна зазначити, що галузь телекомунікацій є висококонкурентною через сукупність факторів, включаючи технологічний прогрес, дерегуляцію, конвергенцію послуг, глобалізацію та попит споживачів. Постачальники повинні продовжувати впроваджувати інновації та адаптуватися до мінливих умов ринку, щоб залишатися конкурентоспроможними в цій динамічній галузі.

Розглянемо галузь телекомунікацій України станом на початок дії військового стану. За даними Національної комісії з електронних комунікацій (комісії регулювання зв'язку та інформатизації), в Україні здійснюють діяльність 3 оператора мобільного зв'язку (умовно – Vodafone, Life, Київстар), які надають послуги голосової телефонії та інтернет-зв'язку 3G, 4G (рис. 1) [2].

*Забезпеченість активними ідентифікаційними телекомунікаційними картами мережі рухомого (мобільного) зв'язку на 100 жителів

Рис. 1. Забезпеченість споживачів рухомим (мобільним) зв'язком на 100 жителів*
за регіонами станом на 31.12.2021

Послуги фіксованої телефонії здійснює практично монопольно "Укртелеком" з показниками проникнення, наведеними на рис. 2 [3].

Рис. 2. Забезпеченість населення фіксованим телефонним зв'язком
у розрахунку на 100 жителів за регіонами станом на 31.12.2021*

Також на ринку присутні декілька тисяч різного розміру та організаційно правових форм провайдерів та операторів фіксованого широкосмугового доступу.

Як ми бачимо, найбільш конкурентним ринком у галузі телекомунікацій на початок військового стану був ринок фіксованого Інтернет-доступу.

На ринку телекомунікацій також присутні декілька магістральних операторів з власними оптико-волоконними мережами масштабу країни та взаємоз'єднаннями з міжнародними операторами. Мережі цих операторів прокладені по своїм географічно різним маршрутам, що є фактором безпеки взаємоз'єднань.

Після року воєнних дій можна зробити наступні висновки.

В галузях телекомунікацій, де спостерігалась низька конкуренція, наприклад, мобільний зв'язок, послуги були гіршої якості або були відсутні взагалі на протягом тривалого часу (в деяких локаціях – до тижня).

В галузях телекомунікацій, де спостерігався високий рівень конкуренції, провайдери послуг досить швидко усували пошкоджені мережі, знаходили технічні рішення та оперативно їх впроваджували для забезпечення зв'язку під час блекаутів.

Ще одне явище на ринку телекомунікацій воєнного часу – це вихід на наш ринок глобального провайдера супутникового Інтернет-зв'язку STARLINK. Завдяки цьому стало взагалі можливим використання БПЛА та іншої високотехнологічної зброї.

Як ми бачимо з вищевикладеного, висока конкуренція в телекомунікаційній галузі позитивно впливає на надійність та безпеку телекомунікаційних послуг в надзвичайних ситуаціях та воєнний час. З одного боку, конкуренція може спонукати компанії до більш швидкого впровадження нових технологій та розширення спектру послуг, що може поліпшити доступність до інформації та комунікації в кризових ситуаціях, з іншого боку – висока конкуренція забезпечує високу надлишковість мереж та споруд телекомунікацій та спонукає провайдерів більш оперативно усувати пошкодження та інші інциденти.

1. Грибіненко О.М. (Гапєєва О.М.). Міжнародна економічна безпека в контексті сталого розвитку: Монографія 434 с. / Грибіненко О.М. (Гапєєва О.М.). Дніпро: Середняк Т.К., 2020. 434 с.

2. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку [Електронний ресурс] – Режим доступу до ресурсу: https://nkrzi.gov.ua/index.php?r=site/index&pg=149&language=uk.

3. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку [Електронний ресурс] – Режим доступу до ресурсу: https://nkrzi.gov.ua/index.php?r=site/index&pg=148&language=uk

УДК 004
DOI: 10.31733/17-03-2023-549-551

Володимир ГНЕДЮК
науковий співробітник
Українського науково-дослідного
інституту спеціальної техніки
та судових експертиз, м. Київ

ІНФОРМАЦІЙНА БЕЗПЕКА – ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Інформаційна безпека є надзвичайно важливим елементом національної безпеки, особливо в контексті зростання кількості кібератак та кіберзлочинності, яка може негативно вплинути на військову, економічну та соціальну сфери діяльності держави.

У сучасному світі інформаційні технології стали не тільки надзвичайно корисними, але й небезпечними інструментами, що можуть використовуватися з метою злочинної діяльності та ворожих дій проти інших держав. Кібератаки можуть призвести до витоку конфіденційної інформації, відключення критичних інфраструктурних систем, викрадення грошей, а також до відстеження та моніторингу діяльності громадян та державних структур.

У зв'язку з цим, захист інформаційної безпеки важливий як для держави в цілому, так і для кожного громадянина окремо. Зокрема, державні структури повинні бути готовими до відповіді на кібератаки та розробляти ефективні механізми захисту від них, а громадяни повинні знати про можливі небезпеки в інтернеті та використовувати безпечні методи