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

збереження своїх даних та особистої інформації.

Отже, інформаційна безпека є важливим елементом національної безпеки, який вимагає уваги та захисту, щоб забезпечити стійкість держави та захист громадян від кіберзагроз [1, с. 51].

Україна зосереджує зусилля на захисті своєї інформаційної інфраструктури та кібербезпеці. Деякі технології та методи захисту інформації, які використовуються в Україні:

Шифрування: Шифрування є одним з найпоширеніших методів захисту інформації. Україна використовує шифрування для захисту конфіденційної інформації від несанкціонованого доступу. У 2018 році Україна приєдналася до Всесвітнього співтовариства з криптографії, що дозволяє Україні брати участь у розробці стандартів шифрування та інших криптографічних технологій.

Захист від шкідливих програм: Україна використовує спеціальні програмні засоби, щоб захистити свої комп'ютерні системи від шкідливих програм. Для цього використовуються антивірусні програми, програми захисту від зламу та інші програмні продукти.

Моніторинг та аналіз безпеки мереж: Україна використовує різні програмні та апаратні засоби для моніторингу та аналізу безпеки мереж. Ці засоби дозволяють виявляти потенційні загрози безпеці та реагувати на них вчасно.

Регулярне навчання та підвищення кваліфікації персоналу: Україна зосереджує зусилля на навчанні та підвищенні кваліфікації персоналу з питань кібербезпеки та захисту інформації. Національний кіберцентр України регулярно проводить тренінги та семінари для працівників відповідних органів влади та інших зацікавлених сторін.

Використання багатофакторної аутентифікації: Багатофакторна аутентифікація – це метод захисту інформації, який використовує більше одного виду ідентифікації для підтвердження права доступу до системи. Україна використовує багатофакторну аутентифікацію для захисту своїх комп'ютерних систем та мереж від несанкціонованого доступу.

Міжнародне співробітництво: Україна підтримує міжнародне співробітництво у сфері кібербезпеки. Уряд України підписав численні угоди з іншими країнами з питань кібербезпеки та бере участь у роботі міжнародних організацій, таких як ООН та ЄС, з питань кібербезпеки та захисту інформації [2, с. 74–75].

Усі ці технології та методи захисту інформації допомагають забезпечувати високий рівень інформаційної безпеки в Україні. Однак, також необхідно звернути увагу на те, що українські компанії та організації повинні приділяти належну увагу захисту своїх інформаційних ресурсів та підвищенню кваліфікації своїх фахівців у галузі кібербезпеки.

Недостатній рівень інформаційної безпеки може призвести до витоку конфіденційної інформації, порушення правил регулювання відомчих секретів та значної матеріальної шкоди. Тому важливо не тільки використовувати сучасні технології захисту інформації, але й забезпечувати належний рівень кваліфікації фахівців, а також регулярно проводити аудити та тестування систем захисту на вразливість [4, с. 98].

Під час воєнного стану в Україні приймаються зміни до нормативно-правових актів, що враховують реалії війни. Ці зміни стосуються регулювання інформаційних правовідносин, зокрема заборони поширення інформації, що має суспільно-небезпечний характер, технічного фіксування інформації, посилення відповідальності за поширення забороненої інформації, врегулювання процесуальних дій щодо вилучення інформаційних даних.

Законопроєкт про кримінальну відповідальність за незаконну фото- та відеозйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану було ухвалено Верховною Радою. Також зміни до Кримінального процесуального кодексу спрощують проведення слідчих дій та тимчасових доступів до речей і документів, дозволяючи слідчому фіксувати комп'ютерні дані на місці обшуку.

Крім того, була посилено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції згідно з законом України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» [3, с. 153].

Сучасні військові конфлікти яскраво демонструють, що інформація може бути ефективною зброєю масового враження. Тому необхідно створити ефективний механізм, який забезпечуватиме державну інформаційну безпеку та дотримання прав людини, а

водночас не порушуватиме свободи та демократію. Українці дуже цінують свої права на свободу та справедливість, захищаючи їх навіть своїм життям.

Для створення ефективної системи інформаційної безпеки необхідно використовувати три логічні складові:

технічну – створення та функціонування всіх необхідних технічних систем;

політичну – державна політика повинна бути спрямована на забезпечення інформаційної безпеки;

правову – всі елементи повинні бути оформлені у відповідні нормативно-правові акти.

Створення інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства та людини. У час війни захист інформаційної безпеки є пріоритетним, оскільки від нього безпосередньо залежить безпека суспільства та людини. В цей період публічно-правовий захист виходить за межі традиційного регулювання та охоплює приватно-правові відносини [3, с. 154].

Отже, захист інформаційної безпеки є невід'ємною складовою національної безпеки кожної країни. В сучасному світі, де інформаційні технології стають все більш важливими і широко використовуються, захист інформації стає пріоритетним завданням для кожної держави. Збільшення кількості кібератак і кіберзлочинів свідчить про те, що інформаційна безпека стає все більш важливою для забезпечення національної безпеки.

Для побудови ефективної системи інформаційної безпеки в умовах війни необхідно мати комплексну технічну та політико-правову діяльність уповноважених органів, спрямовану на захист держави, суспільства та людини.

1. Бондарчук В. І., Бондарчук О. В. Інформаційна безпека в системі національної безпеки держави. 2019. *Політологічні читання*. №18. С. 50–54.

2. Гінзбург А. І., Семенов В. М. Інформаційна безпека держави: сутність та напрями забезпечення. *Наукові записки Інституту законодавства Верховної Ради України*. №3. 2020. С. 72–79.

3. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2022. С. 150–155.

4. Кулаківська Г. О. Інформаційна безпека України в умовах інформаційної війни. *Науковий вісник Чернівецького університету*. № 951. 2021. С. 97–101.

УДК 004+159.595
DOI: 10.31733/17-03-2023-551-553

Володимир ГНЕДЮК
науковий співробітник

Олена ГОРУН
головний науковий співробітник
Українського науково-дослідного
інституту спеціальної техніки
та судових експертиз, м.Київ

ІНФОРМАЦІЙНА БЕЗПЕКА – ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ. РОЗВИТОК КРИТИЧНОГО МИСЛЕННЯ ЯК СПОСІБ ПРОТИДІЇ ПРОПАГАНДІ

На сьогоднішній день у людства існує упередженість, що людина суттєво відрізняється від тварин. Але наявність однієї спільної риси спростовує багато тверджень з цього приводу. Мова йде про вбивство. У тваринному світі існує чимало агресивних видів тварин, які здатні вбивати собі подібних, але причини скоєння вбивства у тварин суттєво відрізняються від людських. Люди - єдиний вид, який здатен вигадати історію, аби вважати, що за допомогою вбивства інших людей існує спосіб врятувати собі життя. 24 лютого 2022 року увесь світ був свідком демонстрації ілюзорних імперіалістичних амбіцій росії. Під гаслом «На захист батьківщини!» російська федерація розпочала масштабні вбивства українців, ставлячи перед собою мету виправдання своїх агресивних намірів нібито наявною загрозою життю і безпеці росіян. У веденні агресивної війни російської федерації