УДК 004.056
DOI https://doi.org/10.32782/2524-0374/2023-12/100

СУЧАСНИЙ СТАН КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО ПЕРІОДУ

THE CURRENT STATE OF CYBER SECURITY IN UKRAINE IN THE LANGUAGES OF THE WAR PERIOD

Колосовський Є.Ю., к.ю.н.,
завідувач кафедри кримінального судочинства та аналітичної діяльності
Державний податковий університет

Круць Е.М., студентка І курсу магістратури
Навчально-науковий інститут економічної безпеки та митної справи Державного податкового університету

У статті розглядається стан кібербезпеки України в період введеного воєнного стану. Виділено, що на сьогоднішній день після повномасштабного вторгнення російських військ на територію України бойові дії в нашій країні ведуться не лише на передовій. Саме тому слід констатувати, що в інформаційному просторі держави, зокрема мережі Інтернет відбувається справжня інформаційна війна. При цьому наголошено, що кібершпигунство та кібертероризм в економічній сфері держави є не менш небезпечним, адже націлюються на підрив економічних відносин, провокацію соціального невдоволення. Таким чином, пріоритетне завдання щодо формування в країні сучасної та ефективної системи протидії кіберзагрозам є запорукою забезпечення невід'ємної складової національної безпеки України – інформаційної безпеки на належному рівні. Проаналізовано нормативно-правове регулювання кібербезпеки в сучасних умовах та надані пропозиції щодо внесення змін з метою удосконалення існуючих нормативно-правових актів у даній сфері. Так, до основних нормативних джерел, що регулюють питання забезпечення належного рівня кібербезпеки в України слід віднести Конституція України та спеціалізовані Закони України. Відмічено, що сьогодні війна в інформаційному просторі, завдає не менших збитків, аніж на полі бою, оскільки країна-агресор застосовує інтернет-технології задля дезінформації міжнародного суспільства щодо повномасштабного вторгнення в Україну, пропагування ворожих ідей, антиукраїнських наративів тощо. Виокремлено основні спроби кібератак починаючи від 24 лютого 2022 року. Визначено, що для ефективного протистояння наявним загрозам в кіберпросторі, потрібні належні умови та узгоджена взаємодія суб'єктів забезпечення кібербезпеки в державі. Реалізація даного положення в практичній площині можлива при застосуванні дієвого механізму в сфері кібербезпеки України. У підсумку визначено, що сучасний стан кібербезпеки України в умовах воєнного періоду є предметом серйозного поглибленого аналізу та глибокого розуміння важливості захисту кіберпростору в умовах воєнної загрози. Здатність країни в умовах військових конфліктів ефективно захищати свої інформаційні ресурси стає ключовим фактором для забезпечення національної безпеки та економічного розвитку.

Ключові слова: кібербезпека, кіберзлочинність, інформаційна безпека, воєнний стан, злочинність у сфері інформаційних технологій.

The article examines the state of cybersecurity in Ukraine during the imposed martial law. It is highlighted that, at present, after a full-scale invasion of Russian forces into Ukrainian territory, military actions in our country are not only taking place on the front line. Therefore, it should be noted that a real information war is taking place in the country's information space, particularly on the Internet. It is emphasized that cyber espionage and cyber terrorism in the country's economic sphere are equally dangerous as they target the undermining of economic relations and provocation of social dissatisfaction. Thus, the priority task in forming a modern and effective system to counter cyber threats in the country is the guarantee of ensuring an integral component of Ukraine's national security – information security at an appropriate level. The regulatory and legal regulation of cybersecurity in modern conditions is analyzed, and suggestions are provided for amendments to improve existing legal acts in this area. Among the main normative sources regulating the issue of ensuring an adequate level of cybersecurity in Ukraine, the Constitution of Ukraine and specialized laws of Ukraine should be considered. It is noted that today, the war in the information space inflicts no less damage than on the battlefield, as the aggressor country utilizes internet technologies for disinformation of the international community regarding the full-scale invasion of Ukraine, promotion of hostile ideas, anti-Ukrainian narratives, and more. The main attempts of cyber attacks starting from February 24, 2022, are highlighted. It is determined that for effective resistance to existing threats in cyberspace, proper conditions and coordinated interaction of subjects ensuring cybersecurity in the state are necessary. The implementation of this provision in practical terms is possible with the application of an effective mechanism in the field of cybersecurity in Ukraine. In conclusion, it is stated that the current state of cybersecurity in Ukraine during wartime is the subject of a serious in-depth analysis and a profound understanding of the importance of protecting cyberspace in the face of military threats. The country's ability to effectively defend its information resources becomes a key factor in ensuring national security and economic development.

Key words: cybersecurity, cybercrime, information security, martial law, crime in the field of information technology.

Постановка проблеми. На сьогоднішній день після повномасштабного вторгнення російських військ на територію України бойові дії в нашій країні ведуться не лише на передовій. Безумовно, такі фактори як введення воєнного стану в державі, втрата домівок, майна, загибель близьких людей, вимушена зміна місцепроживання – всі ці явища мали негативний вплив на поведінку та безпосередню свідомість громадян країни. Втім, окрему увагу привертають на себе саме інформаційні атаки, які безпосередньо направлені на підрив ментального здоров'я українців. Саме тому слід констатувати, що в інформаційному просторі держави, зокрема мережі Інтернет відбувається справжня інформаційна війна.

Україна під час широкомасштабної агресії зустрічається з різними видами кібератак та кіберзлочинів. Країна-агресор прагне заблокувати надання електронних послуг наслідком чого є непоодинокі випадки порушення прав громадян. Порушуються цілісність та конфіденційність персональних відомостей, здійснюються фішингові атаки, провокується інформаційно-психологічний натиск на людей. Слід зауважити, що кібершпигунство та кібертероризм в економічній сфері держави є не менш небезпечним, адже націлюються на підрив економічних відносин, провокацію соціального невдоволення. Таким чином, пріоритетне завдання щодо формування в країні сучасної та ефективної системи протидії кіберзагрозам є запорукою забезпечення невід'ємної складової національної безпеки України – інформаційної безпеки на належному рівні.

Метою статті є аналіз сучасного стану кібербезпеки України, причин та умов поширення вчинення кримінальних правопорушень в даній сфері в умовах воєнного стану, що був запроваджений в державі.

Питання протидії кіберзлочинності неодноразово привертало увагу вчених. Так, можна виділити наступних дослідників: О. М. Бандурка, І. Р. Березовська, В. В. Василевич, Б. М. Головкін, С. О. Гнатюк, О. П. Дзьобань,

Б. А. Кормич, В. В. Марков, В. С. Цимбалюк, О. К. Юдін та інші.

Виклад основного матеріалу. Відповідно до положень ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», під терміном «кібербезпека» слід розуміти захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1]. Втім, аналіз публікацій за темою дослідження свідчить про наявну наукову дискусію, яка характеризується відсутністю єдиного підходу щодо визначення ознак, які характеризують кібербезпеку. До прикладу, В. Н. Фурашев пояснює поняття «кібербезпеки» як стан здібностей людини, народу та держави загалом, стосовно запобігання та усунення, свідомого, прямого негативного впливу інформації [2, с. 164].

Д. О. Ширяєв відзначає, що «кібербезпека є складною та багатогранною проблемою, яка вимагає спільних і постійних зусиль усіх зацікавлених сторін. Працюючи разом над розробкою найкращих практик, обміном інформацією та інвестуванням у нові технології, ми зможемо краще захистити себе та свою цифрову інфраструктуру від кіберзагроз» [3, с. 602].

У свою чергу, Л. М. Бєлкін, Ю. Л. Юринець, М. Л. Бєлкін, Є. В. Криволап виокремлюють, що «кібербезпека є окремим випадком загального поняття безпеки інформації, але такої інформації, яка обертається у кіберпросторі. При цьому причиною підвищеної уваги саме до кіберзагрозам і кібербезпеки є дедалі зростаюча роль обігу інформації в комп'ютерних системах і електронно-комунікаційних мережах» [4, с. 80].

Так, можемо відзначити, що кібербезпека може бути охарактеризована наступними аспектами:

– як система спеціальних суб'єктів, які забезпечують комп'ютерну безпеку, разом із методами та засобами, які вони використовують, а також як система взаємопов'язаних організаційних, технічних та правових заходів, що впроваджуються цими суб'єктами;

– як рівень захищеності електронних інформаційних ресурсів держави у кіберпросторі від ризиків зовнішнього впливу, а також як система виявлення та протистояння різним формам зовнішнього втручання через інформаційні системи;

– як система елементів комп'ютерної безпеки, які взаємодіють між собою, комплектуються та розгортаються відповідно до єдиного плану з метою забезпечення безпеки інформаційно-телекомунікаційних систем;

– як рівень захищеності важливих і життєвих інтересів людини, громадянина, а також суспільства та держави загалом, за якого можливе безперешкодне збирання, використання та зберігання інформації;

– як здатність держави запобігати та уникати спрямованого негативного впливу. Виходячи з вище окресленого, зазначимо, що кібербезпека являє собою основу національної безпеки України, яка складає стан захищеності країни, суспільства, системи публічного управління в кібернетичному просторі шляхом утворення легітимних механізмів забезпечення кібербезпеки публічного управління.

До основних нормативних джерел, що регулюють питання забезпечення належного рівня кібербезпеки в України слід віднести Конституція України та Закони України, зокрема: «Про національну безпеку України», «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних мережах». Вказані нормативно-правові акти визначають загальні засади національної безпеки держави, принципи зовнішньої та внутрішньої політики у даній сфері, а також особливості захисту державних інформаційних ресурсів та інформації з обмеженим доступом.

Також слід звернути свою увагу і на підзаконні нормативні акти у цій сфері. До таких слід віднести Укази Президента України: «Про Стратегію національної безпеки України» [5], «Про Стратегію кібербезпеки України» [6], «Про Стратегію інформаційної безпеки» [7]. Затвердженими стратегіями передбачаються перспективи щодо створення максимально вільного, безпечного, стабільного, відкритого кіберпростору в інтересах забезпечення прав людини в Україні.

Загальновідомо, що обсяг інформаційних ресурсів постійно збільшується і все більше користувачів працюють та спілкуються без територіальних обмежень. Кіберзлочинці використовують складну методику для одержання доступу до ресурсів, викрадення даних та для саботування роботи компаній щоб вимагати кошти.

До основних об'єктів кібератак слід віднести: діяльність уряду, збройних сил, правоохоронних органів, ЗМІ (комунікаційні системи державної, комунальної та інших форм власності, в яких обробляються інформаційні ресурси та які використовуються в інтересах органів державної влади, правоохоронних та військових формувань); ядерна та хімічна промисловість (комунікаційні та технологічні системи критичних інфраструктурних об'єктів держави: до таких відносять українські АЕС, та перелік національних хімічних підприємств країни); транспортні та комунікаційні мережі (комунікаційні системи, які застосовуються для задоволення суспільних потреб або здійснення правовідносин в сферах електронних державних послуг, електронного документообігу, електронної комерції та електронного урядування); національна та фінансова системи (національні комунікаційні системи фінансових установ держави, окремою категорією є банківські мережі).

Кіберпростір, прийнято розглядати як середовище для можливих злочинних дій в сфері несанкціонованого доступу до конфіденційних відомостей, збоїв в діяльності програмного забезпечення та порушення режиму функціонування автоматизованих програм.

Реальний стан сьогодення, це те, що сьогодні фахівці фіксують збільшення кількості кіберінцидентів та кібератак на державні інформаційні резерви та об'єкти критичної інфраструктури України.

Державна Служба спеціального зв'язку та захисту інформації повідомляє, що від 24 лютого 2022 року, за допомогою засобів виявлення вразливостей та реагування зв'язку на кібератаки та кіберінциденти було виявлено та досліджено 24 млрд подій в інформаційному просторі. Збільшився об'єм зареєстрованих та опрацьованих кіберінцидентів від 65 до 120, порівнюючи з попередніми періодами та даними [8].

Слід констатувати, що головною метою хакерів є: знищення відомостей інформаційних мереж, кібершпіонаж та порушення загальнодоступності інформаційних мереж.

Спеціалісти Державного центру кіберзахисту стверджують, що відбулось помітне збільшення поширення неправомірного, шкідливого програмного забезпечення. Кількість атак з високим рівнем критичності виросла майже в 4 рази, а кількість зареєстрованих кіберінцидентів з високим рівнем критичності близько на 130%. На протязі цих місяців, у 35 разів збільшилась кількість критичних подій інформаційної безпеки, джерело яких – IP-адреси, що належать росії [8].

Починаючи з 2018 року починає свою роботу Ситуаційний центр забезпечення кібербезпеки при Службі безпеки України. Цей уряд створився при допомозі Північноатлантичного альянсу. Технічне обладнання і програмне забезпечення діяльності Центру було надано в межах здійснення першого рівня Угоди про здійснення Трастового фонду України – НАТО щодо питань кібербезпеки. На основі Ситуаційного центру, сформувалась система управління подіями інформаційної безпеки. Це надає

можливість швидко виявляти, реагувати і прогнозувати загрози в сфері національного кіберпростору [9].

Необхідно зауважити, що з початком війни, стало відомо про дуже велику кількість кібератак на українські ресурси. Важко навіть повірити в те, перш ніж повномасштабно ввійти на територію нашої держави – розпочався напад російської армії хакерів. Дані агентства Reuters США та загалом Європейський союз, в офіційному порядку, звинуватили росію у повномасштабному кібернападі, що зміг порушити діяльність інтернет-сервісу Viasat. Дана подія відбулась за годину до нападу російських військ 24 лютого 2022 року. Це знищило "десятки тисяч" супутникових терміналів [10].

Відповідно до даних MIT Technology Review – атакування російських хакерів платформи Viasat – один з найбільш болючих моментів за період війни. Так, один з живих прикладів того, що кібератаки можуть конкретно направлятися і розраховуватися за часом, для того щоб посилити ворожість збройних сил, через порушення і загалом знищення розвинутих технологій [11, с. 46]. Ворожа програма, стерла всі дані модемів та маршрутизаторів Viasat, результатом чого стало абсолютне відключення пристроїв. Також 23 березня 2022 року країна-агресор намагалася нанести потужну кібератаку на державні установи України із застосуванням мало знайомих та шкідливих програм. Одна з таких програм Cobalt Strilke Beacon, програма яка здійснює безповоротне враження всієї системи у випадку, якщо перейти за посиланням та відкрити її.

Не можна не згадати спробу атаки угрупування хакерів Strontium. Дане угрупування намагалося сконцентрувати власні сили на одержанні доступу до усіх комп'ютерних мереж в Україні. Вони планували здійснити забезпечення фізичного вторгнення росії на тактичному рівні а також викрасти і знешкодити всі конфіденційні дані. В квітні 2022 року Державна Служба спеціального зв'язку та захисту інформації екстренно попередила про масове поширення електронних посилань, що називалось «Військові злочини РФ. Htm» [8].

Слід відмітити, що переважна частина українського населення, нехтує рекомендаціями військових, а саме Міністерства оборони України, яке завжди попереджає на власному офіційному інтернет-сайті, про те, що соціальні мережі, надають адміністрації сайту можливість збирати відомості про персональні дані без відома окремих осіб, адже немає можливості відстежити збір належної інформації в таких системах [12].

Поширення фотографій на сторінках соціальних мереж з військовою технікою, із зброєю, з локацією місцезнаходження одного чи кількох військових публікувались і, на жаль публікуються, і на сьогодні. Дуже вірним, хоч і з затримкою, було введення кримінальної відповідальності за вказані дії.

Саме попередження – це однин з видів боротьби зі злочинами кіберсфері. Саме цей вид забезпечує заходи правового, економічного, ідеологічного, технічного, правового, організаційного, криптографічного та програмного характеру. Україна налічує багато платформ для інформування суспільства стосовно шахрайських схем та засобів і для того щоб не стати жертвами кібершахрайства. На спеціальних ресурсах, роз'яснюють правила кібербезпеки і дають поради громадянам.

Варто підкреслити, що в першу чергу потрібно додержуватись правил кібергігієни в боротьбі з фейками: вивчати тільки перевірені, офіційні джерел, а не сумнівні пости соціальних мереж. В цей же час, слід пам'ятати, що серед умов воєнного часу, навіть найбільш надійні медіа-офіційні особи можуть припускатися помилок. Знайшовши важливі новини, потрібно знайти або дочекатись їх підтвердження [13, с. 5].

Стосовно діпфейків, тут ситуація складніше, адже це підробка відео, на якому може бути публічна особа, проголошуючи якусь промову. Наприклад це може бути відеозвернення Президента України – Володимира Зеленського нібито про капітуляцію. Дана методика машинного навчання застосовується для того, щоб заплутати слухачів та підірвати бойовий дух громадян держави. При такій ситуації варто звертати увагу на головні ознаки:

– мерехтіння кадру;
– сповільнене кліпання очима;
– неприродні ознаками зовнішності;
– незвичайний тон виступу.

На сьогодні Україна має сильну армію фахівців в ІТ середовищі, які здійснюють захист інтересів в інформаційному середовищі.

Спеціалісти ІТ, реалізують успішне атакування сервісних додатків та регіональних підрозділів державної влади Росії. На території росії вони знаходяться в закритому контурі, однак ІТ-армії Укріни вдається їх вражати. Таким чином, аналіз теми показав, що ефективність забезпечення кібербезпеки, вимагає комплексного вирішення, сконцентрованих дій як на національному так і на міжнародному рівнях для підготовки, реагування, прогнозування та відновлення інцидентів зі сторони органів влади.

Висновок. Сучасний стан кібербезпеки України в умовах воєнного періоду є предметом серйозного поглибленого аналізу та глибокого розуміння важливості захисту кіберпростору в умовах воєнної загрози. Здатність країни в умовах військових конфліктів ефективно захищати свої інформаційні ресурси стає ключовим фактором для забезпечення національної безпеки та економічного розвитку.

Дуже дієве та кваліфіковане протистояння загрозам національній безпеці в кіберпросторі – реальне тільки при відповідних умовах, щодо комплексного застосування всієї наявності правових інструментів для найкращого забезпечення кібербезпеки. Це відноситься до пунктів, які діють за всіма відповідними елементами державного управління та на всіх рівнях руху інформації. Можна стверджувати, що найбільший ефект відображається в абсолютній взаємодії суб'єктів забезпечення кібербезпеки України. Це можна здобути шляхом застосування цілісних та ефективних системних механізмів, адміністративно-правових методик та різних методів, за допомогою яких реалізується державна політика в секторі забепечення кібербезпеки, яких складових частин національної безпеки України.

Отже, важливість вдосконалення та посилення систем кіберзахисту стає очевидною, і вимагає комплексних заходів як на рівні технічної інфраструктури, так і на рівні законодавства, навчання та свідомості громадян. Забезпечення кібербезпеки в умовах воєнного періоду вимагає постійного моніторингу, адаптації до нових загроз та вдосконалення стратегій захисту.

ЛІТЕРАТУРА

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 17.08.2022 р № 2163-VIII. *Відомості Верховної Ради*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 25.12.2023 р.)

2. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.

3. Ширяєв Д.О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів.* Вінниця, 2023. С. 600–602.

4. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law»*, *3*(64). 2022. С. 78–86.

5. Указ Президента України «Про Стратегію національної безпеки України» від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення 25.12.2023 р.).
6. Указ Президента України «Про Стратегію кібербезпеки України» від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 25.12.2023 р.).
7. Указ Президента України «Про Стратегію інформаційної безпеки» від 28.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 25.12.2023 р.).
8. Державна Служба спеціального зв'язку та захисту інформації. *Офіційна веб-сторінка.* URL: https://cip.gov.ua/ua (дата звернення 25.12.2023 р.).
9. Служба безпеки України. *Офіційна веб-сторінка.* URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky (дата звернення 25.12.2023 р.).
10. Війна росії проти України почалася з кібернападу на супутники. за годину до вторгнення були знищені «десятки тисяч» терміналів Viasat -itc.ua.ITC.ua. URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-zkibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki (дата зверненн 25.12.2023 р.).
11. Яковлєв П. Державне регулювання у сфері захисту кіберпростору як складник забезпечення інформаційної безпеки України. *Customs Scientific Journal.* 2020. № 1. С. 43–48.
12. Міністерство оборони України. *Офіційна веб-сторінка.* URL: https://www.mil.gov.ua/ (дата звернення 25.12.2023 р.).
13. Шестак Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану. *Інформаційна безпека та комп'ютерні технології.* Ценральноукраїнський національний технічний університет, Кропивницький, 2022. С. 5–6.
14. Климчук О. О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3. С. 75–83.