особистою інформацією та відповідального використання технологій.

Шляхи реалізації підвищення кіберсвідомості та кіберкультури повинні включати проведення інформаційно-просвітницьких кампаній, навчання основам кібергігієни та безпечної поведінки в Інтернеті, а також заохочення розвитку кіберкультури [3]. Тобто треба розроблювати інформаційні матеріали, які будуть доступні та зрозумілі для різних груп населення. Використання простої мови та наглядних прикладів сприятиме залученню більшої аудиторії. Також важливим є впровадження позитивного підходу до кібербезпеки, де користувачі бачать це не лише як необхідність, але і як частину сучасного, високотехнологічного способу життя, в якому буде усвідомлена важливість дотримання основних правил безпеки. Всі ці аспекти допоможуть не тільки уберегти свою особисту інформацію як інтернет користувача, але й вберегти користувачів від участі в гібридній війні у інформаційному кібер простірі.

Як висновок можно зазначити що підвищення кіберсвідомості та кіберкультури – це інвестиція в безпечне майбутнє України. Це не лише спосіб захистити себе та свої дані від кібератак, але й важливий фактор національної безпеки. Реалізація раніше зазначених шляхів потребує спільних зусиль з боку держави, громадських організацій та всіх громадян України. Тільки спільними зусиллями ми можемо значно підвищити кіберстійкість України та протистояти всім можливим кіберзагрозам.

1. Задубінний А. Стратегія кібербезпеки України: цілі та пріоритети. АрміяInform – Інформаційне агентство АрміяInform. URL : https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/ .

2. Три года после масштабной атаки WannaCry: уровень распространения угрозы не снижается. Malware Protection & Internet Security | ESET. URL : https://www.eset.com/ua-ru/about/newsroom/press-releases/malware/tri-goda-posle-masshtabnoy-ataki-wannacry-uroven-rasprostraneniya-ugrozy-ne-snizhayetsya-ru/.

3. Microsoft назвала масштабную кибератаку тревожным сигналом – BBC News Україна. BBC News Україна. URL : https://www.bbc.com/ukrainian/news-russian-39915638.

УДК 004.738.5:341.31
DOI: 10.31733/15-03-2024/2/367-369

Дарина НІКОЛАЙЧУК
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Юлія СИНИЦІНА
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РОЗВИТОК КІБЕРЗАХИСТУ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

Актуальність розвитку кіберзахисту під час воєнного стану в Україні визначається надзвичайною потребою забезпечення безпеки та захисту інформаційних ресурсів у найбільш напружених та небезпечних умовах. У зв'язку зі збільшенням загроз кібербезпеці в умовах збройного конфлікту, необхідно зосередитися на розробці та впровадженні ефективних заходів з протидії кібератакам та захисту важливих інформаційних структур.

Ситуація в Україні вимагає негайних заходів щодо підвищення кібербезпеки через ризик втрати чутливої інформації та можливість дестабілізації владних структур у воєнний період. Розвиток кіберзахисту в цих умовах стає пріоритетним завданням для забезпечення національної безпеки та військового успіху. Зокрема, потрібно розробляти та впроваджувати нові технології та стратегії кібербезпеки, підвищувати кваліфікацію персоналу з цієї галузі, зміцнювати системи моніторингу та аналізу для виявлення та відвернення кібератак.

Досягнення успіху в цьому напрямку важливо не лише для захисту власних

інтересів, але й для відстоювання демократичних цінностей, підтримки прав людини та стабільності у регіоні. Тому розвиток кіберзахисту під час воєнного стану має велике стратегічне значення для України та її міжнародного статусу.

Протягом тривалого періоду російські спецслужби реалізують складні інформаційні стратегії, спрямовані переважно на порушення національної безпеки та суверенітету України. Дії російських спецслужб націлені на дезінформацію, дестабілізацію суспільства та відшкодування української ідентичності. Шляхом провокацій та впливу на громадську думку вони намагаються послабити український національний дух, спричинити паніку, інститут екстремізму, та загрожувати політично-економічним стабільності України [1].

Ураховуючи цей контекст, забезпечення кібербезпеки для України стає надзвичайно важливою задачею, що потребує комплексного підходу та стратегічних рішень.

Українська політика у цій сфері спрямована на створення надійного національного кіберпростору, що забезпечує відкритість суспільства та безпечність його використання. Важливою метою є збереження незалежності в цифровому просторі та забезпечення захисту національних інформаційних ресурсів від зовнішнього втручання. Стратегія включає в себе різноманітні напрями, включаючи боротьбу з кібертероризмом, зниження вразливості критичних об'єктів, і виконання міжнародних зобов'язань у сфері кібербезпеки. Вибір конкретних заходів залежить від характеру загроз та вимог безпеки життєво важливих інтересів громадян і держави [1].

У воєнний час, ця стратегія стає ще більш критичною, вимагаючи оперативних рішень та ефективних заходів для захисту країни від кібернападів та втручання. У контексті воєнного стану основними стратегічними напрямами забезпечення кібербезпеки в Україні є розвиток державної інформаційної інфраструктури та забезпечення безпечної експлуатації ключових об'єктів цієї інфраструктури. Крім того, важливими є розвиток міжнародного співробітництва у сфері кібербезпеки, згуртування ресурсів та посилення координації між правоохоронними, розвідувальними і контррозвідувальними органами для протидії кібертероризму. Ефективне використання Збройних Сил для адекватної відповіді на кіберзагрози, розробка перспективних науково-технічних напрямків, підтримка вітчизняних виробників у сфері кібербезпеки та адаптація законодавства до стандартів ЄС – це також ключові завдання.

Суть державної політики полягає в забезпеченні балансу між захистом конституційних прав та свобод громадян в інформаційному просторі і виявленням, попередженням та нейтралізацією загроз інформаційній безпеці країни [2]. Це передбачає розвиток нормативно-правової бази, гармонізацію з міжнародним правом і стандартами Європейського Союзу, а також активну взаємодію між державним та приватним секторами на національному і міжнародному рівнях.

Важливою складовою є також протидія дезінформаційним операціям, які намагаються підривати незалежність країни та порушувати її конституційний лад. Ці операції спрямовані на поширення різноманітних форм ворожнечі та тероризму через інформаційний простір [3]. Отже, в умовах воєнного стану в Україні розвиток кіберзахисту стає надзвичайно важливим завданням з урахуванням постійних кіберзагроз з боку російських спецслужб та інших агресивних суб'єктів. Основними напрямками забезпечення кібербезпеки в цих умовах є розвиток державної інформаційної інфраструктури, підвищення ефективності міжнародного співробітництва, об'єднання ресурсів та посилення координації між правоохоронними органами для протидії кібертероризму. Зокрема, необхідно активно розвивати новітні технології та використовувати кращі практики для покращення кіберзахисту критичних об'єктів інформаційної інфраструктури. Також важливо підтримувати вітчизняних виробників у сфері кібербезпеки та адаптувати законодавство до стандартів Європейського Союзу.

Забезпечення ефективного кіберзахисту вимагає також підвищення обізнаності громадськості щодо ризиків і загроз у кіберпросторі. Крім того, важливо активно протидіяти дезінформаційним операціям, спрямованим на підрив державності, національної ідентичності та соціальної стабільності.

До основних перспективних напрямів розвитку кіберзахисту під час воєнного стану в Україні, можна віднестти наступні:

Розробка та впровадження інноваційних кіберзахисних технологій: Потрібно інвестувати у дослідження та розробку передових кіберзахисних систем, які враховують специфіку воєнного стану. Це може включати розробку систем шифрування,

інтелектуального виявлення загроз, та адаптивних систем захисту.

Підвищення кваліфікації персоналу та підготовка експертів у галузі кібербезпеки: Необхідно проводити навчальні курси, тренінги та семінари для працівників правоохоронних та військових організацій з питань кіберзахисту. Це допоможе підготувати кваліфікованих фахівців, які зможуть вчасно реагувати на кіберзагрози.

Створення спеціалізованих центрів кібербезпеки: Важливо створити центри, які будуть відповідальні за моніторинг та аналіз кіберзагроз, а також за реагування на інциденти кібербезпеки в умовах воєнного стану.

Міжнародне співробітництво в галузі кібербезпеки: Україна повинна активно співпрацювати з іншими країнами та міжнародними організаціями у сфері обміну інформацією та досвідом щодо кіберзахисту під час воєнного конфлікту.

Забезпечення резервування та відновлення інформаційних систем: Важливо розробити та впровадити плани резервування та відновлення інформаційних систем, що дозволить відновити роботу критичних інформаційних ресурсів у найкоротший термін після кібератаки або інциденту.

Проведення свідомості та просвітницьких заходів: Важливо надавати інформацію громадськості про потенційні кіберзагрози та методи їх запобігання. Це допоможе залучити громадян до заходів кібербезпеки та створить атмосферу зростаючої уваги до цих питань у суспільстві.

Загалом, розвиток кіберзахисту під час воєнного стану в Україні вимагає комплексного підходу, спрямованого на створення надійного інформаційного простору та ефективну відповідь на кіберзагрози з метою захисту національних інтересів та забезпечення безпеки громадян і держави.

1. Синиціна Ю.П. Інформаційна безпека умовах військовий стану. Сучасні пріоритети розвитку України: економічна та інформаційна безпека: зб. матеріалів Всеукр. наук.-практ. конф. Дніпро: ДДУВС, 2023. С. 103–108.

2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник. Львів: «Магнолія 2006», 2018. 320 с.

3. Безуглий Д., Інформаційна безпека України: огляд останніх тенден- цій. Фізико-математична освіта, вип. № 2(16), 2018. С. 13–17 с.

УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/369-370

Egor NIKULIN
Olga PECHKOVSKAYA
students of group TI-222

Lucia GUZHUMAN
PhD, Associate Professor

Serghei OHRIMENCO
DsC, Professor

(Laboratory of Information Security,
Academy of Economic Studies,
Chisinau, Moldova)

NEW CHALLENGES OF CYBER SECURITY

The report examines new cyber security challenges in an ever-changing threat landscape. These include, most notably, an increased number of software abuses (e.g., crypto-ransomware) targeting mobile applications and communications and developed using artificial intelligence and machine learning tools [1],[2],[3].

A separate and poorly researched group of security threats is represented by situations when supercomputers will be used on the defending and attacking sides. Currently, such scenarios have been analysed only at the theoretical level, but their implementation is already possible in the confrontation in cyberspace between individual countries and their groups. The uniqueness of the situation lies in the following [4]: