- технологія «25-ий кадр», заборонена міжнародним законодавством;
- замовчування важливих подій.

На жаль, усі ці методи впливають на психіку людей і суспільства загалом таким чином, що люди вважають, що думки та переконання, нав'язані ЗМІ, є їхнім життєвим досвідом і власними висновками.

Контент-аналіз новин російської федерації проти України та інтернет-ресурсів дозволив підкреслити, що щоденні матеріали на порталах є агресивними та очевидно спотвореними. Журналісти дозволяють собі використовувати емоційно забарвлену лексику у своїх матеріалах про Україну, її владу, армію та активістів; заголовки в такому контенті не є винятком. Наразі наприклад на одному з російських сайтів розміщений заголовок «Чому нацизм відродився в Україні, а не в Німеччині», де зазначається: «Потрібно відверто визнати: з одного боку, вчасно не добили українських нацистів, а потім вибачили їх на догоду якимсь сьогохвилинним політичним віянням. З іншого боку – заграліся у дружбу народів. Мовляв, не може один братній народ ненавидіти та винищувати інші братні народи. Отже, народ не може, а ось окремі його представники – цілком» [4].

Проаналізувавши заголовки з новин про події в Україні на російських сайтах, можна поділити їх на кілька так званих «пропагандистських груп». Особливо це помітно на новинних порталах «Правда.Ru» та «Московський комсомолець». Згідно з дослідженням, використовуються такі відомі методи пропаганди: навішування ярликів, апеляція до влади, демонізація ворога, спрощення фактів, побутовий наратив, емоційний резонанс, анонімний авторитет, гра в «приналежність» до російського народу, «загальна думка». Ці методи дають людям відчуття приналежності до «великої і могутньої» росії та її «братнього народу». У такий спосіб автори матеріалів нав'язують суспільству певні цінності, ідеї та програми.

1. До 5-річчя від початку збройної агресії Російської Федерації проти України. URL : https://cutt.ly/DHwbsKQ (дата звернення: 11.04.2022).

2. Маркова М. В., Марков А. Р. Інформаційно-психологічна війна як нова загроза здоров'ю населення України: реальність небезпеки та напрями протидії. Здоров'я України. Неврологія. Психіатрія. Психотерапія. 2016. № 1 (36). С. 51-53. URL : http://irbis-nbuv.gov.ua.cgi-bin.irbis_nbuv.cgiirbis_64.Psmno_2016. (дата звернення: 25.09.2023).

3. Денисюк С.Г., Корнієнко В.О. Імідж України у внутрішньо і геополітичних контекстах сучасності. Житомир-Київ-Краків: ФОП Євенюк О. О., 2014. Вип. 4. С. 93-100. URL : http://nbuv.gov.ua/UJRN/Spup_2014_4_13. (дата звернення: 25.09.2023).

4. Почему нацизм возродился на Украине, а не в Германии. RGRU. URL : https://rg.ru/2022/04/06/pochemu-nacizm-vozrodilsia-na-ukraine-a-ne-v-germanii.html (дата звернення: 25.09.2023).

УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/362-364

Владислав МІЛЕНІН
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Сергій ПЕТРЕНКО
старший викладач кафедри
спеціальної фізичної підготовки
Дніпропетровського державного
університету внутрішніх справ

ПРІОРІТЕТИ ЗАБЕСПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У сучасному цифровому світі кібербезпека стає однією з найбільш актуальних і складних проблем для країн у всьому світі, включаючи Україну. Щодня збільшується кількість кіберзагроз і кібератак, спрямованих на урядові установи, підприємства та громадянське суспільство. У зв'язку з цим забезпечення кібербезпеки стає пріоритетною

задачею для України.

Вступаючи в епоху цифрової трансформації, Україна зустрічається з необхідністю захищати свою інформаційну і кібернетичну інфраструктуру від різноманітних загроз, що включають в себе кібершпигунство, кібертероризм, кібервійну та кіберзлочинність. З урахуванням різноманітності цих загроз, Україна має визначити свої пріоритети у сфері кібербезпеки і впровадити ефективні заходи для їх вирішення. Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека – це 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].

Зростаюча кількість кібератак створює низку серйозних викликів у контексті кібербезпеки України. По-перше, це підвищує ризик недостатньої підготовленості українських органів влади та приватних компаній до відповіді на кіберзагрози. Зловмисники намагаються використовувати вразливості в існуючих заходах безпеки для отримання доступу до конфіденційної інформації або національних ресурсів.

Другим викликом є недостатній рівень координації та співпраці між урядовими органами, приватним сектором та іншими зацікавленими сторонами. Україна потребує посилення співпраці між всіма рівнями влади, щоб ефективно реагувати на кіберзагрози та обмінюватися інформацією про потенційні загрози.

Зокрема, зростаюча кількість кібератак ставить під загрозу економічну стійкість країни, оскільки кіберінциденти можуть призвести до великих втрат для підприємств та бюджету держави. Зловмисники можуть використовувати різноманітні стратегії, включаючи розшифрування даних, вимагання викупу або навіть порушення роботи критичної інфраструктури.

Таким чином, зростаюча кількість кібератак підвищує необхідність в постійному вдосконаленні технологій та стратегій кіберзахисту. Україна повинна вкладати значні зусилля у розвиток сучасних технологій кібербезпеки та навчання кадрів для боротьби з новими формами кіберзагроз.

Україна, подібно багатьом іншим країнам, стикається з великим спектром потенційних кіберзагроз до різних сфер її інфраструктури. Однією з основних сфер, яка потребує найбільшого захисту, є енергетика, з огляду на її стратегічне значення для функціонування країни. Захист енергетичних систем вимагає впровадження високого рівня захисту мереж та систем керування, а також регулярних аудитів безпеки.

Ще однією ключовою сферою є інформаційно-комунікаційні технології (ІКТ), які потребують надійного захисту від кібератак та захисту конфіденційної інформації. Захист ІКТ-інфраструктури передбачає використання механізмів шифрування, міцних паролів та систем виявлення вторгнень.

Також важливою є захист критичної інфраструктури, такої як транспортні системи, медичні установи та системи водопостачання. Для забезпечення кібербезпеки в цих сферах необхідно проведення оцінки ризиків, розробка планів надзвичайних ситуацій та впровадження ефективних технічних та організаційних заходів безпеки.

У сучасному кіберпросторі України існують різноманітні кіберзагрози, які варіюються від кібератак на критичну інфраструктуру до кібершпигунства та соціального інжинірингу. Зловмисники зосереджують зусилля на пошуку вразливостей активів (систем управління) і розробляють для цього унікальні за своїми властивостями: багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети, що здійснюють розподілені атаки (DDoS) на операційні мережі, виробничі системи, які використовують хмарні сервіси, атаки на ланцюги поставок. З урахуванням розвитку технологій штучного інтелекту найближчими 5-10 роками масштаби та наслідки таких втручань зростатимуть. [2]. Нестримна цифрова активність вимагає постійного вдосконалення заходів безпеки для захисту важливих систем і даних країни. Кібератаки на критичну інфраструктуру, таку як енергетичні системи, транспортні мережі та медичні установи, можуть мати серйозні наслідки для економіки та безпеки суспільства. Зокрема, кібершпигунство та фішинг можуть призвести до розголошення конфіденційної інформації або порушення приватності користувачів.

Для виявлення та запобігання цим загрозам в Україні використовуються різноманітні стратегії та підходи. Однією з них є застосування систем виявлення вторгнень (IDS/IPS), що допомагають виявляти та блокувати незвичайну активність в мережі. Також

створюються кіберсервіси та підтримка інцидентів, що спеціалізуються на виявленні, реагуванні та розслідуванні кіберінцидентів.

Регулярні аудити безпеки є необхідним елементом стратегії забезпечення кібербезпеки в Україні. Вони дозволяють виявляти вразливості та слабкі місця в інформаційних системах та інфраструктурі, що дозволяє приймати вчасні заходи для їх усунення. Крім того, проведення кампаній із кіберосвіти та навчання персоналу щодо безпеки в Інтернеті допомагає підвищити обізнаність користувачів та зменшити ризики кібератак.

Державна влада відіграє надзвичайно важливу роль у забезпеченні кібербезпеки України. По-перше, це включає розробку та впровадження стратегій, політик і нормативно-правових актів, спрямованих на захист країни від кіберзагроз. Документами, що місять принципи формування та реалізації державної інформаційної політики, зокрема пов'язані з протидією деструктивному зовнішньому інформаційному впливу, є Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та плану заходів щодо її реалізації Розпорядженнями Кабінету Міністрів України від 20 вересня 2017 року [3], від 8 листопада 2017 року № 797-р [4] та від 17 січня 2018 року № 67-р [5], а також Укази Президента України від 14 вересня 2020 року № 392/2020 «Про Стратегію національної безпеки України», від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України», від 27 січня 2016 року «Про Стратегію кібербезпеки України» [6; 7; 2] тощо.Ці документи визначають напрямки дій, необхідні для забезпечення безпеки інформаційного простору та інфраструктури.

Другий аспект – це створення та підтримка спеціалізованих організаційних структур, що відповідають за кібербезпеку. До їх функцій входить моніторинг інформаційних потоків, виявлення потенційних загроз, реагування на кіберінциденти та координація дій з іншими зацікавленими сторонами.

Крім того, державна влада активно співпрацює з приватним сектором та міжнародними партнерами для ефективної боротьби з кіберзагрозами. Ця співпраця включає обмін інформацією про загрози, розробку спільних стратегій та заходів, а також координацію дій для забезпечення кібербезпеки на національному та міжнародному рівнях.

Усвідомлення важливості кібербезпеки стає все більш актуальним у сучасному світі, особливо для країн, що переживають активні кіберзагрози, такі як Україна. Забезпечення кібербезпеки стає одним із пріоритетних завдань держави, оскільки це безпосередньо впливає на економіку, національну безпеку та захист особистої інформації громадян. Для успішного забезпечення кібербезпеки України необхідно посилення співпраці між урядом, приватним сектором та міжнародними партнерами, розробка та впровадження комплексних стратегій та заходів захисту, а також постійне вдосконалення технологічних, організаційних, правових аспектів кібербезпеки. Забезпечення кібербезпеки є важливою передумовою для стійкого розвитку країни та збереження її суверенітету у кіберпросторі.

---

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.02.2024)

2. Draft of the Cybersecurity Strategy of Ukraine (2021-2025) (Unofficial English translation) URL : https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 24.02.2024)

3. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. Урядовий кур'єр. 2017. № 181.

4. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 8 листопада 2017 р. № 797-р. Урядовий кур'єр. 2017. № 217.

5. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Урядовий кур'єр. 2018. № 88.

6. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 р. № 392/2020. База даних «Законодавство України». URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 р. № 96/2016. Урядовий кур'єр. 2016. № 52