СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну гвардію України : Закон України від 13.03.2014 № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18.
2. Про оборону України : Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12
3. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VII. URL: https://zakon.rada.gov.ua/laws/show/389-19
4. Доктрина «Цивільно-військове співробітництво» (СП 9-00(01).01) : затверджена Головнокомандувачем Збройних Сил України від 01.07.2020. URL: https://sprotyvg7.com.ua
5. Цивільно-військове співробітництво: алгоритм ефективної взаємодії громадських організацій та вищих військових навчальних закладів. *Проблеми інженерно-педагогічної освіти*. 2022. № 74. С. 25–31.

ЯХІН РОСТИСЛАВ РУШАНЬОВИЧ
курсант 2 навчального курсу 3 групи

ГОНТАР АНАСТАСІЯ ВАДИМІВНА
курсантка 2 навчального курсу 2 групи Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ МАСОВИХ КІБЕРАТАК З БОКУ АГРЕСОРА

Повномасштабне вторгнення росії на територію України, що триває з 24 лютого 2022 року, перетворило кіберпростір на середовище збройного протистояння. Кібератаки та інформаційно-психологічні операції агресора стали невід'ємними складовими гібридної війни, яка поєднує традиційні військові методи з економічними, інформаційними та кібернетичними засобами впливу. Саме тому інформаційна безпека держави в умовах інтенсивних кібератак є одним із пріоритетних завдань у системі національної безпеки України, що безпосередньо пов'язане з боєздатністю збройних сил та ефективністю системи державного управління.

Гібридна агресія росії проти України характеризується поєднанням кінетичних та некінетичних засобів: збройні удари супроводжуються кібератаками, дезінформаційними кампаніями та інформаційно-психологічними операціями. Тривале інформаційне протиборство є основою насильницького впровадження інтересів агресора, а силовому ресурсу відводиться лише підсилююча роль на окремих етапах збройного конфлікту. Посилення агресії проти суверенних держав передбачає удари по системах державного управління, економіці через ракетні обстріли інфраструктури, кібератаки та пропаганду [1].

Масові кібератаки на українські державні установи та бізнес розпочалися задовго до відкритого військового вторгнення. З початком бойових дій 24 лютого 2022 року їх кількість подвоїлася – з приблизно 200 на місяць до понад 400 [2]. Служба безпеки України у 2020 році зафіксувала 800 кібератак, у 2021 році – близько 2 000, а після початку повномасштабного вторгнення – понад 4 500. Станом на лютий 2023 року СБУ відбила понад 550 атак, при цьому в середньому на добу фіксується понад десять кібератак різних типів [3]. Найбільш поширеними стали DDoS-атаки, злом великих компаній з подальшою крадіжкою інформації та дефейс популярних ресурсів. Під прикриттям масових атак продовжують діяти кіберзлочинці, націлені на державний сектор, банківську сферу, паливно-енергетичний комплекс, наукові установи.

Федеральні спецслужби росії систематично застосовують шкідливе програмне забезпечення – віруси, трояни, програми-вимагачі, хробаки – для ураження державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Типовою методологією кібератак є збір інформації засобами OSINT, використання шкідливого програмного коду, несанкціоноване втручання в державну цифрову інформаційну інфраструктуру. Окремою загрозою залишаються фішингові атаки: лише у 2022 році Національний банк України виявив понад 4 500 фішингових ресурсів, а в першому кварталі 2023 року – вже понад 11 000 шахрайських доменів, переважна більшість яких має російське походження [4].

Сучасний стан загроз вимагає переходу до принципово нових підходів у сфері виявлення та нейтралізації кібератак. Найбільш актуальним завданням у сфері інформаційної безпеки є виявлення вторгнень та атак на автоматизовані системи в умовах кібервійни. Для захисту критичних систем інформаційної інфраструктури застосовуються міжмережові екрани, системи виявлення та попередження вторгнень (IDS/IPS), системи запобігання втраті даних (DLP) та системи управління подіями інформаційної безпеки (SIEM) [2]. Разом з тим традиційні методи, що ґрунтуються на сигнатурному аналізі, мають суттєвий недолік – вони нездатні виявляти нові, раніше невідомі кібератаки, які є причиною глобальних інформаційних катастроф. Перспективним вирішенням є застосування методів глибокого машинного навчання, зокрема рекурентних нейронних мереж архітектури LSTM, які дозволяють виявляти аномальну поведінку контрольованих систем у режимі реального часу з високим рівнем достовірності.

На момент початку гібридної агресії у 2014 році Україна не була готовою до масованої інформаційно-пропагандистської атаки як складової воєнного конфлікту нового покоління; фактично бракувало системи підготовки кадрів у сфері кібербезпеки для потреб збройних сил та сектору безпеки і оборони [1]. Росія застосовує інформаційно-пропагандистський ресурс комплексно, задіюючи широкий спектр каналів – традиційні та інтернет-ЗМІ, соціальні мережі, масштабний інтернет-тролінг – і витрачаючи на це ресурси, неспівмірні з можливостями малих постраднянських країн. Завданням підготовки майбутніх офіцерів є формування здатності розпізнавати інформаційно-психологічні операції противника, критично оцінювати інформаційне середовище та забезпечувати стійкість особового складу до деструктивного впливу.

Ефективна протидія масовим кібератакам потребує реалізації комплексу заходів у тактичному та стратегічному вимірах. В Україні функціонує багаторівнева система кіберзахисту, до суб'єктів якої належать Державна служба спеціального зв'язку та захисту інформації України, СБУ, Департамент кіберполіції Національної поліції, відповідні підрозділи Міністерства оборони та Генерального штабу ЗС України. Організаційно-технічна модель кіберзахисту, затверджена Постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426 передбачає три інтегровані рівні: організаційно-керівний, технологічний та базовий, що забезпечують координацію зусиль між суб'єктами безпеки, моніторинг кіберпростору та відновлення систем після атак [3].

Кібербезпека не може бути досягнута на суто національному рівні – це потребує спільних зусиль приватного сектору та міжнародної координації. У цьому контексті приєднання України 16 травня 2023 року до Центру НАТО з питань співробітництва в галузі кіберзахисту відкрило можливості для обміну досвідом та отримання підтримки у разі кібератак національного масштабу [4].

Отже, забезпечення інформаційної безпеки держави в умовах масових кібератак з боку агресора є комплексним і невідкладним завданням. Кіберпростір перетворився на самостійне середовище воєнних дій, де поєднуються технічні засоби ураження та інформаційно-психологічний вплив. Готовність офіцера до дій в умовах кіберагресії включає розуміння природи гібридних загроз, знання методів виявлення і нейтралізації шкідливого програмного забезпечення, а також здатність підтримувати моральний стан особового складу перед лицем інформаційно-психологічних операцій противника. Системна відповідь на кіберагресію вимагає впровадження сучасних технологічних засобів захисту, удосконалення законодавчої бази та поглиблення міжнародного співробітництва у сфері кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юрчак Ю. М. Підготовка майбутніх офіцерів до протидії негативному інформаційно-психологічному впливу агресора в умовах інформаційної війни. Педагогічні науки: теорія, історія, інноваційні технології. 2024. № 1–2 (135–136). С. 64–81.

2. Лебідь О. В., Кіпоренко С. С., Вовк В. Ю. Виявлення кібератак та підвищення інформаційної безпеки на основі технології нейронних мереж в умовах кібервійни. Наука і техніка сьогодні. 2023. № 1(15). С. 238–256.

3. Мануілов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. № 1(44). С. 154–167.

4. Федієнко О. П. Загрозливі тенденції використання державою-агресором шкідливого програмного забезпечення в умовах правового режиму воєнного стану. Інформація і право. 2023. № 3(46). С. 142–153.