МУДРА Світлана В'ячеславівна,
кандидат педагогічних наук, доцент, завідувач кафедри мовної підготовки Київського інституту Національної гвардії України
ЛОСЮК Тарас Тарасович,
курсант, командир 3 відділення 112 навчальної групи факультету ЗДБ Київського інституту Національної гвардії України

КІБЕРБЕЗПЕКА І ВІЙСЬКОВА КОМУНІКАЦІЯ: ВИКЛИКИ ТА ЗАГРОЗИ

Завдання забезпечення національної безпеки та оборони сучасного суспільства неможливо уявити без врахування кіберпростору. Сьогодні практично кожен аспект суспільства, включаючи військову сферу, сильно залежить від інформаційних технологій та кіберпростору. Це охоплює комунікації, управління ресурсами, зв'язок між військовими підрозділами, важливі інфраструктурні об'єкти, енергетичні системи та багато інших аспектів. Інформаційні технології відіграють важливу роль у веденні війни та в оборонній стратегії. Ми розглянемо виклики та загрози, які стикаються військові сили у сфері кібербезпеки.

Виклики військової комунікації в кіберпросторі:

1. *Збільшення обсягу інформації:* Сучасна військова комунікація вимагає швидкого обміну великими обсягами інформації. Це може створювати труднощі у контролі над даними та їх захисті від кіберзлочинців. Під час бойових операцій військовий персонал в обласному командному центрі надсилає великі обсяги даних, включаючи звіти про стан військ, важливі стратегічні дані та супутникові зображення, до центральної військової бази. Захист цієї інформації є критично важливим, оскільки її перехоплення або зміна може спричинити серйозні проблеми для військового управління.

2. *Анонімність та псевдоніми:* Вороги можуть використовувати анонімні акаунти та псевдоніми для розповсюдження дезінформації та проведення атак на військові системи з використанням хакерських технологій. Атакуюча група може створити анонімний акаунт в соціальній мережі та використати його для поширення фейкових новин про надходження ворожого війська на територію країни. Ця дезінформація може призвести до паніки в суспільстві та неконтрольованого реагування з боку військового керівництва.

3. *Кібершпигунство:* Різні країни та групи можуть використовувати кібершпигунство для отримання важливої військової інформації, такої як плани операцій, розташування військ, технічні характеристики. Кібершпигунство або комп'ютерний шпіонаж – несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, з

застосуванням шкідливого програмного забезпечення, включаючи «троянських коней» і шпигунських програм [2]. Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств звичайними шпигунами («кротами»), а також хакерами. З недавніх пір кібершпигунство включає також аналіз провідними спецслужбами (ЦРУ, Моссад, ФСБ) зокрема за спостереженням цифрового сліду поведінки користувачів соціальних мереж (Повідомлення, друзі, фотографії, відео тощо), таких як Facebook, «ВКонтакте», Twitter тощо з метою виявлення екстремістської, терористичної чи антиурядової діяльності, закликів збору на мітинги проти влади.

Заходи кібербезпеки стають надзвичайно важливими через зростаючу залежність військових структур від інформаційних технологій та кіберпростору. Зокрема, військове керівництво використовує ці технології для координації операцій, обміну конфіденційною інформацією та контролю над стратегічними ресурсами.

Зловмисники, у тому числі терористичні групи та хакери, виявляють все більший інтерес до вразливостей у військових мережах і системах. Їхня здатність проводити різноманітні кібератаки, включаючи розповсюдження шкідливого програмного забезпечення, перехоплення комунікацій та дезінформацію, становить серйозну загрозу для ефективності та безпеки військових операцій.

Загрози військової комунікації в кіберпросторі:

1. *Кібератаки:* Кібератаки представляють собою спрямовані дії на військові мережі та інформаційні системи з метою завдання шкоди або заважання їхньому нормальному функціонуванню. Ці атаки можуть включати в себе такі види атак, як деніал-сервіс атаки (намагання перевантажити систему запитами, щоб зупинити її роботу), використання шкідливих програм (включаючи віруси, троянські програми і черв'яки), атаки на інфраструктуру (наприклад, на важливі комунікаційні вузли) [5].

2. *Фішинг і соціальна інженерія:* Зловмисники, які використовують фішинг і соціальну інженерію, намагаються отримати доступ до військових систем, введучи в оману військових працівників [4]. Це може включати в себе відправку фішингових листів, що видавались за легітимні повідомлення, або маніпулювання людьми через соціальні інтеракції з метою отримання паролів, логінів та інших важливих даних.

3. *Дезінформація та вплив на громадську думку:* Зловмисники можуть поширювати дезінформацію через військові комунікаційні канали з метою спричинення паніки, створення хаосу або впливу на вирішення військового керівництва. Ця інформація може бути неправдивою або спотвореною та може використовувати різні медійні форми.

4. *Кібертероризм:* У контексті кібертероризму, кібератаки можуть бути спрямовані на різні об'єкти та системи, включаючи критичну інфраструктуру, електронні комунікації, фінансові установи, військові системи та інші об'єкти. Наприклад, це може включати атаки на електроенергетичні мережі, банківські системи, аеропорти, транспортні системи, медичні заклади тощо [2].

Метою кібертерористів є створення хаосу, паніки та нанесення значних завдань матеріальних або інших збитків суспільству або державі. Вони можуть використовувати кіберагресію для втручання в політичні процеси, дестабілізації суспільства, чи навіть для розповсюдження ідеологічної або релігійної пропаганди.

Захист від кібертероризму є надзвичайно важливим завданням для держав та міжнародних організацій, і вимагає спільних зусиль у сфері кібербезпеки, розвідки та правопорядку для запобігання та реагування на кібератаки, які можуть мати серйозні наслідки для безпеки та стабільності.

У статті розглянуті важливі аспекти кібербезпеки та її вплив на військову комунікацію в сучасному світі. Основні виклики, які виникають у цій області, включають збільшення обсягу інформації, анонімність та псевдоніми, а також кібершпигунство. Загрози для військової комунікації в кіберпросторі включають кібератаки, фішинг і соціальну інженерію, дезінформацію та кібертероризм.

Зростаюча залежність військових структур від інформаційних технологій та кіберпростору робить кібербезпеку надзвичайно важливою для забезпечення національної безпеки та оборони. Зловмисники, у тому числі терористичні групи та хакери, становлять серйозну загрозу, і вони активно використовують кібератаки та інші методи для завдання шкоди та нанесення збитків.

Список використаних джерел

1. Служба безпеки України. Захист інформаційного та кіберпростору. Звіт SIEM. URL: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення: 15.09.2023)

2. Brenner, J. (2007). America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. Penguin.

3. Указ Президента України від 30 серпня 2017 року № 254/2017 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року „Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації“, введеного в дію Указом Президента України від 13 лютого 2017 року № 32»»

4. Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. Rand Corporation.

5. Ліпкан В.А. Кібербезпека як складова національної безпеки України / В.А. Ліпкан // Інформаційні технології в економіці, менеджменті і бізнесі : Проблеми науки, практики і освіти : Зб. наук. праць VIII Міжнар. наук.-256 практ. конф. — Ч. 2. — К. : Вид-во Європ. ун-ту, 2003. — С. 443–453.