Цимбал Єлизавета Андріївна
курсант 212 навчальної групи ННІ № 1 НАВС, рядовий поліції

Науковий керівник:
Буренко Олег Володимирович
викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, підполковник поліції

ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Ми живемо в епоху інформаційного суспільства, де інформаційні технології та телекомунікаційні системи проникають у всі сфери людського життя та державного управління. На сьогоднішній день жертвами хакерів можуть стати не тільки окремі особи, але й цілі держави. За наслідками та ефективністю використання кіберзброї, яку науковці все частіше порівнюють з зброєю масового знищення, кібербезпека стає однією з ключових проблем, яка викликає серйозне занепокоєння. І чим стрімкіше розвивається людство в інформаційних технологіях, тим більше зростає необхідність в захисті інформаційно-телекомунікаційних систем. Оскільки програмне забезпечення та автоматизовані системи стають дедалі більш вразливими до кібератак, тож не дивно, що уряди та суспільство активно працюють над пошуком найефективніших методів захисту особистих даних та Інтернет-ресурсів від цих загроз.

В Україні поняття «кібербезпека» вперше було використано у 2007 році [1], спочатку в контексті потреби «розробки та впровадження національних стандартів та технічних регламентів з використання інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, включно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність». З 2016 року під кібербезпекою в Україні розуміється стан захищеності життєво важливих інтересів людини, громадянина, суспільства та держави в кіберпросторі [2]. Згідно з Законом України [3], кібербезпека - це захищеність життєво важливих інтересів людини, громадянина, суспільства та держави під час використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

В умовах воєнного стану захист суспільства від деструктивного інформаційного впливу з боку держави агресора та ряду терористичних організацій, які задіяні в процесі дестабілізації нашої країни, а також від інших негативних інформаційних факторів, які руйнують вітчизняний інформаційний простір, необхідно уточнити форми та методи забезпечення інформаційної безпеки громадян.

Стратегія кібербезпеки України [2] визначає пріоритетні заходи у забезпеченні кібербезпеки сектору безпеки й оборони, а саме:

– Створення і розвиток сил, засобів та інструментів для можливої відповіді на агресію у кіберпросторі, що може бути використана як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист).

– Проведення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі.

– Розвиток підрозділів кібербезпеки та кіберзахисту ЗСУ.

– Утворення єдиного підрозділу для забезпечення кібербезпеки та кіберзахисту ЗСУ на стратегічному, оперативному та тактичному рівнях.

– Розширення науково-виробничого потенціалу та системи підготовки спеціалістів з кібербезпеки для потреб органів сектору безпеки і оборони України.

Значна кількість загроз інформаційної безпеки створює наступні ризики:

– Можливість використання інформаційних технологій та механізмів для реалізації ворожих актів агресії проти громадян.

– Неправомірна діяльність в інформаційному просторі з метою дестабілізації суспільства.

– Незаконне використання інформаційних ресурсів інших держав.

– Маніпулювання інформацією з метою спотворення сталих моральних, етичних та культурних цінностей.

– Використання інформаційної інфраструктури для поширення ідей та теорій, що сприяють міжрасовій та міжнаціональній ворожнечі, а також пропаганди ненависті, дискримінації та насильства.

Глобальна кібербезпека мусить спрямовувати зусилля на захист та безпеку мережі з використанням наступних рівнів захисту інформації:

1) Попередження – доступ до бази даних та технологій надається лише авторизованому персоналу з відповідними спеціальними навичками;

2) Виявлення – забезпечення раннього виявлення злочинів та зловживань, навіть при наявності захисних механізмів;

3) Стримування – мінімізація збитків у разі вчинення правопорушень незалежно від заходів їх запобігання та виявлення;

4) Відновлення – забезпечення повного відновлення даних за наявності документованого та перевіреного плану відновлення [4].

Таким чином, для запобігання та вирішення проблем в галузі кібербезпеки, необхідно постійно проводити діагностування систем шляхом проведення спеціальних тестів, використання спеціалізованого обладнання та залучення кваліфікованих фахівців, які зможуть усунути причини можливих вразливостей. Також важливо пам'ятати, що ми всі знаходимося в одному великому мережевому просторі, тому навіть звичайний співробітник або військовослужбовець може стати жертвою будь-якого вірусу, що може призвести до зараження на всіх рівнях. Тому, одним із ключових аспектів кібербезпеки є проведення навчань з працівниками з метою запобігання та протидії кібератакам.

Список використаних джерел:

1. Стратегія національної безпеки України, затверджена Указом Президента України від 12.02.2007 No105/2007в редакції Указу Президента України від 8.06.2012 року No 389/2012. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/105/2007.

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 No 96.Офіційний вісник України. 2016. № 23.

3. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю.Є. Максименко, В. М. Желіховський. Київ: КНТ, 2020. 280 с.

Shaets E.O.
Cadet of the Faculty of Training Specialists for Criminal Police Units, Donetsk State University of Internal Affairs

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

SOCIAL ENGINEERING AS A METHOD OF SHAPING PEOPLE'S CONSCIOUSNESS

Social engineering employs psychological manipulation techniques to shape behavior and beliefs, a tactic evident throughout history in various contexts like politics and marketing.