КІБЕРВІЙНА В УКРАЇНІ

Дикий О.В.

кандидат юридичних наук, доцент
декан факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

У зв'язку з військовою агресією російської федерації проти України 24 лютого 2022 року було введено правовий режим воєнного стану в України. Варто зазначити, що першими були саме масові DDoS-атаки на державні сайти України, банківську систему, ще 23 лютого 2022 року, тобто за день до повномасштабного вторгнення та обстрілів українських міст. Вбачається, що цілю таких кібератак була саме дестабілізація державних та приватних інституцій, вплив на суспільство з метою посіяти панічні настрої.

У війні XXI століття кіберфронт виявися одним із серйозних напрямків активних дій, що безумовно пов’язано із цифровізацією обох сторін війни. Звернемося до дефініції терміну кібервійна. Американський експерт у галузі кібербезпеки Р. Кларк, пропонує так трактування: «Кібервійна – дії однієї національної держави з проникненням у комп'ютери чи мережі іншої національної держави для досягнення цілей завдання шкоди чи руйнування» [1].

Вітчизняний експерт О. Мережко пропонує таке визначення: «Кібервійна – використання Інтернету та пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави» [2].

У Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII складових. Наприклад, кібероборона – це сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

У цьому контексті досить цікаво провести певну аналогію між кібервійною та війною в «реальному» середовищі. Тут хочемо звернути увагу на мобілізаційний потенціал. Так, з моменту вторгнення російської федерації на територію України з перших днів Міністерством цифрової трансформації було створено Telegram канал покликаний масово долучати людей до атак на різні ресурси російської федерації (https://t.me/itarmyofukraine2022). Безумовно він не є ключовим у системній протидії агресору, однак створює серйозні проблеми для противника. Так, за повідомленням із ЗМІ, російські системи постійно стикаються із труднощами функціонування, що дозволяє розпорошувати сили противника на кіберфронті. Вбачається, що в подальшому підготовка мобілізаційного

потенціалу для кіберфронту є однією із пріоритетних. Це пов'язано, в першу чергу, із сучасними умовами ведення війни та їх видозміненням (застосування кібератак). Підготовка таких фахівців повинна здійснюватися для всіх здобувачів освіти в межах галузі знань 12 «Інформаційні технології» у закладах освіти, до того ж до відповідних стандартів освіти повинні бути внесенні відповідні зміни. Як свідчить кількість учасників вказаної групи, до лав кіберармії можна мобілізувати близько 250 тис. осіб (станом на 19.05.2022).

Крім того серед учасників кіберфронту, що стала на захист України після початку повномасштабної війни з росією, об'єдналися наступні групи професіоналів та активістів:

- Досвідчені міжнародні IT-професіонали в галузі кібербезпеки (як представники приватних компаній, так і представники відповідних підрозділів західних спецслужб та підрозділів кібернетичних військ на кшталт британської GIC – Government Information Cell);
- Досвідчені вітчизняні-фахівці в галузі кібербезпеки;
- Українські професіонали в інших галузях IT, що долучилися до кібернетичного фронту як волонтери;
- Існуючі групи фахівців у галузях OSINT (наприклад, Informnapalm) та протидії ворожим дезінформаційним кампаніям (наприклад, StopFake), що сформувалися ще з самого початку агресії Росії у 2014-2015 роках р. та вже зарекомендували себе у боротьбі із ворогом;
- Умотивовані кіберактивісти без спеціальних фахових знань в царині IT, що долучилися до кібернетичного фронту інформаційної війни (поширення правди про події в Україні, участь у пропагандистських кампаніях, розрахованих на населення країни-загарбника, контрпропаганда – боротьба із російськими фейками та дезінформаційними ресурсами в соціальних мережах та в цілому на просторах Інтернету).

Вказане свідчить про значний потенціал саме мобілізаційної складової у активних військових кібердіях.

Також українська сторона використовує краудсорсингові технологій проти ворога на прикладі боту єВорог. Вказаний напрям є одним із новаторських у сучасному світі, так як дозволяє збирати та використовувати інформацію про пересування сил противника фактично в «реальному часі» з детальним описом кількості особового складу та відповідної техніки.

Одним із напрямів кібервійни є протидія пропаганді російської федерації, що направлена на – визначення мародерів армії окупантів через аналіз поштових відправлень та інформування їх родичів через соціальні мережі тощо, а також використання штучного інтелекту для розпізнавання обличчя вбитих солдатів російської федерації та інформування їхніх родичів.

Вказане свідчить про наявний значний напрям подальших наукових досліджень комплексного характеру, що направлений на вивчення феномену

кібервійни, ролі кіберфронту в активних бойових діях та значення мобілізаційного потенціалу кібер фахівців в обороні держави тощо.

Список використаних джерел:

1. Richard A. Clarke and Robert K. Knake»Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010). 2011. 320 p.
2. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). Політичний менеджмент. URL: https://web.archive.org/web/20111007185753/http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.

ЛЮДСЬКИЙ ФАКТОР ЯК ОДИН ІЗ ВИДІВ ВРАЗЛИВОСТЕЙ В КІБЕРБЕЗПЕЦІ

Кравцов О.О.

студент 1-го курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Питання про захист інформаційних інфраструктур, є одним з важливих питань для вирішення, як цивільними підприємствами, так і державою в цілому.

Один із аспектів надання якісного захисту інформаційній інфраструктурі являється протистояння внутрішнім загрозам. Будь-яка інформаційна інфраструктура, яка навіть має найновіші програмно-технічні засоби захисту, все ще опрацьовується людиною, що дає злочинцям, дуже велику вразливість, яку вони можуть використовувати для своїх цілей через соціальну інженерію.

Соціальна інженерія – це термін, який використовується для широкого спектру шкідливих дій, що здійснюються через взаємодію людей. Він використовує психологічні маніпуляції, щоб обманом змусити користувачів зробити помилки безпеки або роздати конфіденційну інформацію[1].

Такі вразливості можливо віднести до внутрішніх загроз до інформаційної інфраструктури. Внутрішні загрози – це загрози, що виникають через користувачів із законним доступом до інформаційної інфраструктури.

Такі користувачі використовують цей доступ зловмисно чи ненавмисно для заподіяння шкоди бізнесу. Внутрішні загрози не обов'язково трапляються через працівників підприємства, вони також можуть трапитися через колишніх співробітників, підрядників або партнерів, які мають доступ до систем або даних організації.

Можна виділити 4 внутрішні загрози:

1) Пішаки – це працівники, які маніпулюють зловмисною діяльністю, часто ненавмисно, за допомогою фішингу або соціальної інженерії. Будь то несвідомий працівник, який завантажує зловмисне на свою робочу станцію, або