3. Виграти війну і не програти демократію: чи зможе Україна впоратися з цим завданням? *Детектор медіа.* URL: https://cs.detector.media/law-and-money/texts/185519/2023-07-05-vygraty-viynu-i-ne-prograty-demokratiyu-chy-zmozhe-ukraina-vporatysya-z-tsym-zavdannyam/.

4. Загрози та виклики демократії у воєнний час: думки експертів. *UPLAN.* URL: https://uplan.org.ua/news/zahrozy-ta-vyklyky-demokratii-u-voiennyi-chas-dumky-ekspertiv/.

Софія БАРТОШ,
курсант 302 н.г. навчально-наукового інституту № 1 Національної академії внутрішніх справ,
Науковий керівник:
кандидат юридичних наук, старший викладач кафедри тактичної підготовки навчально-наукового інституту № 3 Національної академії внутрішніх справ
Богдан ЛІЩУК

КІБЕРБЕЗПЕКА УКРАЇНИ В УМОВАХ ВОЄННОЇ АГРЕСІЇ

Російська агресія проти України супроводжується не лише військовими, але й кіберзасобами. Ще задовго до повномасштабного вторгнення росія посилила кібератаки на держоргани, оборонно-промисловий комплекс, інфраструктурні об'єкти, ІТ-мережі та ЗМІ в Україні. Кібероборотьба й кіберзахист стали одними із ключових елементів гібридної війни.

Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають дошкульних ударів у відповідь. Сьогодні війна в інформаційному просторі, завдає не менших збитків, аніж на полі бою, оскільки країна-агресор застосовує інтернет-технології задля дезінформації міжнародного суспільства щодо повномасштабного вторгнення в Україну, пропагування ворожих ідей, антиукраїнських наративів тощо. Виокремлено основні спроби кібератак починаючи від 24 лютого 2022 року. Визначено, що для ефективного протистояння наявним загрозам в кіберпросторі, потрібні належні умови та узгоджена взаємодія суб'єктів забезпечення кібербезпеки в державі [1].

Найбільше страждають від кібератак державні установи, банки та фінансові організації, інтернет-магазини, ІТ-компанії, бізнес, який працює з персональними даними клієнтів, виробничі компанії та стартапи. Проаналізувавши статистику за останніх два роки війни можна сказати те, що кожна українська компанія повинна бути

напоготові та заздалегідь оцінити вразливість, щоб забезпечити системи від кіберінцидентів і технологічних збоїв. Яскравим прикладом як кібератака може призвести до руйнівних наслідків є знищення ІТ-інфраструктури мобільного оператора Київстар внаслідок кібератаки, яка була здійснена 12 грудня 2023 року [2]. Крім того були ще масові кібератаки на «Дія», «Нафтогаз», збій в системі «Шлях», а також Моно банку і це лише мала частина з понад 4000 атак. Минулого року, наприклад, СБУ викрила та заблокувала російську змову зловмисного програмного забезпечення, яке намагалося проникнути в критично важливі українські системи за допомогою мобільних пристроїв Android, захоплених у українських сил на полі бою [3]. Не слід також забувати те, що переважна частина українського населення, нехтує рекомендаціями військових, а саме Міністерства оборони України, яке завжди попереджає на власному офіційному інтернет-сайті, про те, що соціальні мережі, надають адміністрації сайту можливість збирати відомості про персональні дані без відома окремих осіб, адже немає можливості відстежити збір належної інформації в таких системах [2]. Поширення фотографій на сторінках соціальних мереж з військовою технікою, із зброєю, з локацією місцезнаходження одного чи кількох військових публікувались і, на жаль публікуються, і на сьогодні. Дуже вірним, хоч і з затримкою, було введення кримінальної відповідальності за вказані дії. Саме попередження – це одни з видів боротьби зі злочинами кіберсфері. Саме цей вид забезпечує заходи правового, економічного, ідеологічного, технічного, правового, організаційного, криптографічного та програмного характеру. Україна налічує багато платформ для інформування суспільства стосовно шахрайських схем та засобів і для того щоб не стати жертвами кібершахрайства. На спеціальних ресурсах, роз'яснюють правила кібербезпеки і дають поради громадянам.

Крім того, відповідно до Закону України від 5 жовтня 2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України» де крім основних засад встановлено також ст. 4 «Об'єкти кібербезпеки та кіберзахисту»:

Об'єктами кібербезпеки є: 1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об'єкти критичної інфраструктури.

Об'єктами кіберзахисту є: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або

які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Об'єкти кіберзахисту у сукупності складають критичну інформаційною інфраструктуру і підлягають внесенню до державного реєстру об'єктів критичної інформаційної інфраструктури. Порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджується Кабінетом Міністрів України.

Також слід додати, що у ст. 6 «Об'єкти критичної інфраструктури» Закону України «Про основні засади забезпечення кібербезпеки України» перераховані всі об'єкти інфраструктури наприклад здійснюють діяльність та надають послуги у галузях енергетики, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторі, виконують функції комунальних, аварійних та рятувальних служб, служб екстреної допомоги населенню.

В цілому, кібербезпека України в умовах воєнного періоду є серйозною проблемою, яка потребує постійної уваги та комплексних заходів з боку держави, приватного сектора та громадян. Тільки спільними зусиллями можна ефективно протистояти кіберзагрозам та захистити інформаційний простір України, що забезпечить безпеку в державі та громадян. Досвід, який ми здобуваємо в боротьбі з ворогом, робить наших кіберспеціалістів лідерами галузі на світовому ринку. Крім цього, починає формуватися попит на українські освітні проєкти серед фахівців за кордоном. Із цього можемо зробити висновок, що галузь кіберзахисту у нашій державі й надалі активно зростатиме та залучатиме нові таланти, і настане час, коли ми зможемо повноцінно поділитися набутим знаннями зі світом.

Список використаних джерел

1. Кібербезпека в Україні. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

2. Міністерство оборони України. URL: https://www.mil.gov.ua.

3. Кібербезпека в інформаційному суспільстві. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf.

4. Закону України від 5 жовтня 2017 року № 2163-VIII Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.