вона здатна створити умови для стійкого розвитку країни.

Список використаних джерел

1. Возний В. І. Антикорупційна політика в Україні: навч.-метод. посіб. Тернопіль: ТНЕУ, 2013. 241 с. URL: http://dspace.tneu.edu.ua/retrieve/14165/%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf (дата звернення: 27.03.2024).
2. Державна податкова служба України: Антикорупційне законодавство України. URL: https://tax.gov.ua/diyalnist-/zapobigannya-proyavam-korupts/antikoruptsiyne-zakonodavstvo-ukraini/ (дата звернення: 27.03.2024).
3. Антикорупційна стратегія на 2021–2025 роки. URL: https://nazk.gov.ua/wp-content/uploads/2022/08/Antykoruptsijna-strategiya-na-2021-2025-rr.pdf (дата звернення: 28.03.2024).
4. Закон України «Про запобігання корупції» від 14.10.2014 р. № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18/conv#n239 (дата звернення: 28.03.2024).
5. Денис Малюська: Україна продовжує здійснювати антикорупційні реформи під час війни. URL: https://minjust.gov.ua/news/ministry/denis-malyuska-ukraina-prodovjue-zdiysnyuvati-antikoruptsiyni-reformi-pid-chas-viyni (дата звернення: 28.03.2024).

Відімська Катерина Ігорівна
Старший викладач кафедри суспільних комунікацій та регіональних студій,
факультету міжнародних відносин, політології та соціології.
Одеський національний університет імені І. І. Мечникова

ВИКЛИКИ ТА ВІДПОВІДІ ЗАГРОЗАМ КІБЕРБЕЗПЕЦІ: ДОСВІД ТУРЕЧЧИНИ

У сучасному цифровому світі питання кібернетичної безпеки та інформаційної війни стають все більш актуальними для країн у всьому світі, включаючи і Туреччину. Зростання залежності від інформаційних технологій відкриває безпрецедентні можливості для інновацій та розвитку, але одночасно і створює нові виклики і загрози для національної безпеки та стабільності. У цій статті автор досліджує сучасний стан кібернетичної безпеки в Туреччині, виокремивши ключові аспекти інформаційної війни та заходи, які вживаються для їх протидії. Вивчення цих питань допоможе краще зрозуміти вплив кіберзагроз на сучасне турецьке суспільство та здійснити аналіз можливих шляхів вирішення цих проблем для забезпечення національної безпеки та

стійкості країни.

Кібербезпека - це галузь інформаційної безпеки, що займається захистом комп'ютерних систем, мереж і даних від кіберзагроз, які можуть призвести до неправомірного доступу, руйнування або зламу інформації, а також до знищення або перешкоджання нормальному функціонуванню інформаційних систем. Кібербезпека включає в себе заходи технічного, організаційного та правового характеру для захисту від кібератак, виявлення і реагування на них, а також для відновлення систем після інцидентів. Основні аспекти кібербезпеки включають захист мереж, захист даних, кіберінфраструктури та інформаційних систем, а також розвиток політики та законодавства в галузі кібербезпеки [1, с 46].

У зв'язку зі зростанням кількості кібератак у всьому світі, Туреччина не залишається осторонь. Зловмисники використовують різноманітні методи атак, щоб отримати доступ до конфіденційної інформації, завдати шкоди інфраструктурі та системам критично важливого рівня. Це створює загрозу для національної безпеки та економічного розвитку країни. Туреччина, як і багато інших країн, також стикається з проблемою інформаційної війни. Дезінформація та пропаганда через різноманітні інформаційні канали, включаючи соціальні медіа та традиційні ЗМІ, можуть маніпулювати громадською думкою та підривати довіру до державних інституцій. Критично важливі інфраструктури, такі як енергетика, транспорт, банківська система тощо, можуть бути мішенями кібератак. Недостатній рівень кібербезпеки в цих секторах може призвести до серйозних проблем для функціонування країни.

Туреччина визначається в рамках Vision 2023 цілями, встановленими національною кібербезпекою Міністр транспорту та інфраструктури Абдулкадір Уралоглу Національна стратегія кібербезпеки та План дій турецької галузі кібербезпеки повідомив, що вони прагнуть зайняти перше місце на міжнародному рівні та стати брендом в галузі кібербезпеки на міжнародній арені. Міністр Абдулкадір Уралоглу сказав: "З усвідомленням того, що кібербезпека є невід’ємною частиною нашої національної безпеки, ми продовжуємо працювати в координації з усіма відповідними зацікавленими сторонами, щоб захистити наші активи в кіберпросторі, особливо нашу критичну інфраструктуру, від загроз та зменшити можливі наслідки кіберінцидентів" [5].

Головними стратегічними цілями у сфері кібербезпеці на 2023 рік Туреччина визначила вісім пунктів:

1. Захист критичної інфраструктури та підвищення протидій кібератакам (Kritik Altyapıların Korunması ve Mukavemetin Artırılması)
2. Розвиток національної продуктивності (Ulusal Kapasitenin Geliştirilmesi)

3. Створення мережи органічної кібербезпеки (Organik Siber Güvenlik Ağı)
4. Безпека нових технологій (Yeni Nesil Teknolojilerin Güvenliği)
5. Боротьба з кіберзлочинністю (Siber Suçlarla Mücadele)
6. Розвиток та підтримка місцевих та національних технологій (Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi)
7. Інтеграція кібербезпеки у національну безпеку (Siber Güvenliğin Milli Güvenliğe Entegrasyonu)
8. Розвиток міжнародної співпраці (Uluslararası İş Birliğinin Geliştirilmesi)

Ці заходи спрямовані на покращення рівня кібербезпеки в Туреччині та забезпечення захисту від кіберзагроз для національної безпеки та стабільності країни [6].

Туреччина приділяє велику увагу розробкам національного програмного забезпечення. Країна веде ефективну боротьбу з кіберзагрозами, налагоджуючи національне та міжнародне співробітництво з кібербезпеки через Національний кібер Центр реагування на інциденти. Існує ряд програм для захисту країни, а саме: програма AVCI, розробленої Управлінням інформаційних та комунікаційних технологій, виявляються заражені шкідливим програмним забезпеченням та командні центри управління; програма AZAD знаходить підлеглі комп'ютери з використанням штучного інтелекту; проводяться моніторингові дії щодо відкритих джерел в Інтернеті за проектом KASIRGA. Кібербезпека розробляється повністю з використанням місцевих та національних ресурсів з метою запобігання загрозам DEEP, HUNTERS і протягом останніх 3 років, Туреччина орієнтується на 325 тисяч кібернетиків, що блокують атаку з використанням практики AZAD. За допомогою даних розробок Турецька Республіка запобігла незліченну кількість кібератак за допомогою власного програмного забезпечення. Фактично, згідно з доповіддю Глобального індексу кібербезпеки Міжнародного союзу телекомунікацій, опублікованою в 2023 році, Туреччина піднялася на 23 ранки порівняно з попереднім роком і стала однією з 20 найбезпечніших країн у цій галузі. Менше 1% атак системи безпеки Microsoft зафіксували з Туреччини [3].

Туреччина активно просуває ініціативи щодо підвищення свідомості та освіти населення у галузі кібербезпеки. Це включає проведення кампаній, тренінгів та семінарів для громадськості, а також розвиток навчальних програм у школах та університетах. В країні проводяться саміти з участю міністрів та студентів на тему «штучного інтелекту» і його використання у кібербезпеці.

Туреччина співпрацює з різними країнами у галузі кібербезпеки для обміну інформацією, ресурсами та кращими практиками з метою підвищення рівня кібербезпеки. Туреччина має розвинену співпрацю зі США в галузі кібербезпеки. Обидві країни активно обмінюються інформацією щодо загроз і

викликів у цій області, а також проводять спільні тренування та вправи з кібербезпеки. Також співпрацює з різними країнами Європейського союзу, такими як Німеччина, Франція, Велика Британія та інші. Туреччина є членом НАТО та активно співпрацює з іншими членами альянсу у галузі кібербезпеки. Це включає спільні вправи, обмін інформацією та розвиток загальних стратегій і політик. Співпраця між країнами може відбуватися через різні механізми, включаючи міжнародні договори, обмін інформацією, спільні тренування та вправи, а також через роботу на міжнародних форумах та конференціях з кібербезпеки [7].

Уряд Туреччини приймає нові закони та положення, спрямовані на покращення кібербезпеки та покарання винних у кіберзлочинності. Це включає закони про кібербезпеку, захист особистих даних та боротьбу з кіберзлочинністю.

У 2012 році Кабінетом міністрів було прийняте рішення про створення Ради з кібербезпеці (Siber Güvenlik Kurulu), котра повністю координує підлеглих організацій, відповідає за формування національної стратегії з кібербезпеці [6].

Таким чином, Туреччина, як і багато інших країн, стикається з різноманітними викликами у галузі кібербезпеки, такими як кібератаки, кібершпигунство та кібертероризм. Проте, завдяки розвиненій стратегії, законодавству, співпраці з міжнародними партнерами та підвищенню свідомості громадськості, Туреччина розвивається в напрямку забезпечення ефективного захисту своїх інформаційних систем та інфраструктури. Наслідки кібератак можуть бути серйозними, тому важливо продовжувати зосереджувати увагу на цій проблемі та розвивати ефективні стратегії та заходи для подолання кіберзагроз у майбутньому.

Список використаних джерел

1. Грищук Р.В. Основи кібернетичної безпеки : Монографія / Ю.Г. Даник, Р.В. Грищук ; за заг. ред. проф. Ю.Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

2. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки права НАПрН України»; Національна бібліотека України В.І.Вернадського. К., 2023. №11 (листопад). 300 с.

3. Global Cybersecurity Index 2023. International Telecommunication Union. Development Sector. 2023. P. 172.

4. Global Cybersecurity Outlook 2022. INSIGHT REPORT JANUARY 2022. (2022, January 30). *The World Economic Forum*. Retrieved March 15, 2022.

URL: https://weforum.org. (дата звернення 03.01.2024 р.).

5. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023). URL: https://rayhaber.com/wp-content/uploads/2020/12/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf (дата звернення 03.01.2024 р.).

6. Ulusal Siber Güvenlik Stratejisi 2020-2023. URL: https://rayhaber.com/wp-content/uploads/2020/12/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf (дата звернення 03.01.2024 р.).

7. Zeynep Atım Kurucuk. Navigating the Digital Battlefield: The Role of a Cybercrime Lawyer in Turkey. *Kurucuk & Associates*. URL: https://www.kurucuk.com.tr/post/cybercrime-lawyer-in-turkey (дата звернення 03.01.2024 р.).

Доценко Максим Ігорович
Здобувач третього рівня вищої освіти
кафедри політології та державного управління.
Донецький національний університет імені Василя Стуса
ORCID: 0009-0007-3914-0077

СТАТУС ТОВАРИСТВА ЧЕРВОНОГО ХРЕСТА УКРАЇНИ В УМОВАХ МІЖНАРОДНОГО ЗБРОЙНОГО КОНФЛІКТУ

Повномасштабне вторгнення РФ в Україну актуалізувало питання гуманітарної діяльності та роль, статус і місце окремих акторів у системі гуманітарної допомоги. Товариство Червоного Хреста України (далі – ТЧХУ) є однією з провідних установ з надання гуманітарної допомоги та виконання інших гуманітарних функцій під час міжнародного збройного конфлікту. Інституційна спроможність, здатність Українського Червоного Хреста залучити значні ресурси для гуманітарної діяльності обумовлені його унікальним статусом і роллю допоміжної інституції для держави у здійсненні гуманітарних функцій. Тому важливим є аналіз статусу та місця ТЧХУ в державі та в системі громадянського суспільства.

Незважаючи на наявність значної кількості публікацій про діяльність ТЧХУ, його статус не був предметом політико-правового аналізу. Декілька дисертаційних і монографічних робіт торкалися лише питань створення та розвитку ТЧХУ в історичній ретроспективі [1; 2]. Суто юридичним питанням статусу ТЧХУ також присвячено декілька публікацій [3; 4]. Загальній ролі Національних товариств була присвячена наша публікація [5]. Але досі відсутні комплексні дослідження, які б охоплювали всі аспекти політико-правового