ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЄВРОПЕЙСЬКОМУ СОЮЗІ: ПІДХІД ЄВРОПЕЙСЬКОЇ КОМІСІЇ

Боєр Єлизавета Олександрівна
студентка 2-го курсу факультету міжнародних
економічних відносин та туристичного бізнесу,
Харківський національного Університету імені В. Н. Каразіна
lisaboerrr@gmail.com

За даними Європейської комісії, забезпечення безпеки мережевих та інформаційних систем в Європейському Союзі має важливе значення для підтримки функціонування онлайн-економіки і забезпечення процвітання. ЄС працює по ряду напрямків, щоб сприяти кіберстійкості на вищому рівні [1, с. 141].

У вересні 2017 року Європейська Комісія прийняла реформи, що стосуються кібербезпеки, які ґрунтуються на існуючих інструментах і представляють нові ініціативи для подальшого поліпшення кіберстійкості ЄС, а саме реагування на загрози [4].

Директива з мережевої та інформаційної безпеки (NIS Directive) розробила нову культуру кібербезпеки в ЄС. Завдяки Директиві NIS держави-члени ЄС обмінюються інформацією про інциденти щодо кібербезпеки, а також кращими практиками у сфері боротьби з кіберзлочинністю. Саме група співпраці NIS, створена відповідно до Директиви NIS, зіграла величезну роль у розвитку нової культури кібербезпеки. Ця група підтримує і полегшує стратегічне співробітництво і обмін інформацією між державами-членами ЄС. У наш час співпрацююча група NIS вже досягла чудових результатів для кращої кібербезпеки Європи. Просуваючи співробітництво і обмін інформацією не тільки між державами-членами ЄС, а й між усіма ключовими гравцями у сфері кібербезпеки, а також навчаючись у більш просунутих, або досвідчеих, кібербезпека ЄС значно зміцнилась [1, с. 149].

Наприклад, протягом останніх десятиліть саме банківський сектор був

метою номер один для кібератак, і в результаті в даний час ЄС має найбільш культивовану систему кібербезпеки банківського сектору в дії.

Відповідно до Директиви NIS оператори основних послуг (наприклад, банки, телекомунікаційні компанії, постачальники енергії, лікарні і т. Д.) повинні інформувати національні органи влади, коли вони страждають від кібератак. Директива визначає, про які інциденти повинні повідомляти оператори основних послуг [1, с. 151].

Повідомляючи про напади, вони допомагають іншим, в тому числі владі, дізнатися про характер нападів і про те, як з ними боротися. В даний час ЄС необхідна співпраця і обмін інформацією, а також об'єднання різних навичок і експертів, оскільки інциденти в області кібербезпеки стають все більш витонченими, а економіка і суспільство стають більш цифровими і взаємопов'язаними. Наприклад, гібридні загрози, які можуть варіюватися від кібератак в критично важливих інформаційних системах до зриву критично важливих послуг, таких як постачання енергії або фінансові послуги, можуть привести до підриву довіри громадян до державних установ і вплинути на демократію країн. У той же час важливо вирішувати ці проблеми таким чином, щоб не перешкоджати цифровий трансформації ЄС [2, с. 158].

Цілі Директиви NIS, в більш широкому сенсі, спільної політики і дослідницьких ініціатив в області кібербезпеки, ефективно допомагають ЄС нарощувати його потенціал і стійкість до кібератак. Дійсно, з тих пір як ЄС зробив перший великий крок в області кібербезпеки в Європі, у вигляді Директиви NIS, Європейський Союз дуже швидко просунувся вперед [2, с. 161].

З самого початку існування Європейської Комісії, президент Юнкер, був сповнений рішучості допомогти зміцнити безпеку ЄС, і кібербезпека повинна була стати частиною цього плану. Потім сильну волю і рішучість з цього приводу продемонстрували лідери ЄС [5].

Наприклад, на «Digital Summit 2017» в Естонії, глави всіх країн ЄС обговорили цифровий світ Європи. Саме на цьому саміті вони погодилися, що

кібербезпека повинна вирішуватися в терміновому порядку [4].

В Європі є відмінні експерти з кібербезпеки, в тому числі агентство ЄС з кібербезпеки (ENISA). Крім того, згідно з недавнім опитуванням, ЄС налічує 660 експертних центрів з кібербезпеки по всій території Європейського Союзу.

Але європейська система кібербезпеки залишається дуже фрагментованою. Це перешкода, яку ЄС повинен подолати. Проте, більшість політиків та урядовців країн Європи, вважають що можна перетворити цей виклик в можливість для Європи [5].

Європа має унікальну можливість інвестувати в розширення співпраці і координації між державами-членами ЄС, а також ключовими зацікавленими сторонами ЄС в області кібербезпеки (наприклад, оператори основних послуг) .

Співпрацюючи, об'єднуючи досвід ЄС в області кібербезпеки і розробляючи загальну європейську дорожню карту досліджень та інновацій в області кібербезпеки і промислову європейську стратегію кібербезпеки, Європа може допомогти індустрії кібербезпеки значно зрости, що також призведе до посилення потенціалу кібербезпеки ЄС [3, с. 6].

Саме виходячи з цього, в 2016 році, Європейська комісія підписала з Європейською Організацією Кібербезпеки (ECSO) договірне державно-приватне партнерство (дППП). Перш за все, дППП сприяє структуруванню і координації промислових ресурсів цифрової безпеки в Європі. Воно включає в себе широке коло учасників: виробників компонентів і обладнання, операторів основних послуг і дослідницьких інститутів, об'єднаних під егідою ECSO. ЄС зобов'язався інвестувати до 450 млн. євро в це партнерство [3, с. 8].

В якості наступного амбітного кроку в вересні 2018 року Європейська Комісія запропонувала нову постанову про створення мережі національних координаційних центрів з кібербезпеки і нового Європейського центру компетенції в галузі промислової, технологічної та дослідницької компетенції в області кібербезпеки [3, с. 10-11].

Іншою проблемою для Європи є «нестача фахівців з кібербезпеки». Європейському Союзу потрібно більше людей зі знаннями і навичками в

області кібербезпеки на ринку, як в приватному, так і в державному секторі, щоб вистежувати і реагувати на кіберзагрози. Як показують багато досліджень і доповідей, в Європі не вистачає кваліфікованих фахівців у сфері ІКТ(Інформаційно-комунікаційні технології) і особливо експертів в області кібербезпеки, щоб заповнити зростаюче число вакансій у цій області. Крім того, в пропозиції наступного бюджету ЄС на 2021-2027 роки, робиться наголос на розвиток цифрових навичок, особливо в області кібербезпеки [3, с. 13].

Віце-президент з цифровому єдиного ринку, пан Андрус Ансіп, колишній екс-прем'єр-міністр Естонії, зазначає , що країни з високим рівнем стійкості до кіберзагроз повинні приділяти велику увагу тому, що ми називаємо «кібергігіеной». Подібно до того, як людина використовує певні методи особистої гігієни для підтримки доброго здоров'я і благополуччя, так і правила і запобіжні заходи щодо кібергігієни можуть забезпечити кращий захист користувача від кібератак і витоків даних [4].

Користувачі можуть грати важливу роль в забезпеченні безпеки цифрового суспільства, підвищуючи його проінформованість і практикуючи «кібергігієну». Кваліфіковані фахівці і підприємства в області кібербезпеки повинні співпрацювати і підвищувати проінформованість користувачів про кібербезпеку [5].

Ініціатива ENISA, Європейський місяць кібербезпеки (ECSM) – щорічна кампанія ЄС щодо підвищення обізнаності про кібербезпеку, яка проводиться кожного жовтня по всій Європі [4].

Наразі, вже розглядаються ідеї створення мережі національних координаційних центрів з кібербезпеки і нового Європейського центру в галузі промислової, технологічної та дослідницької компетенції в області кібербезпеки, для вирішення проблеми відсутності навичків і досвіду, щоб об'єднати європейські ресурси і координувати зусилля по зміцненню потенціалу кібербезпеки ЄС і, найголовніше, дати можливість галузям ЄС розробляти конкурентоспроможні по всьому світу продукти та послуги [3, с. 15].

В цілому, Європейський центр компетенції в області кібербезпеки дозволяє розробити платформу для досліджень і інновацій, яка прокладе шлях до безпечної цифрової Європі, вирішуючи всі майбутні проблеми кібербезпеки (штучний інтелект, квант, високопродуктивні обчислення) і використовуються в критичних секторах (наприклад, транспорт, енергетика, охорона здоров'я, фінанси, виробництво, оборона) [5].

Європейська Комісія інвестувала понад 63,5 млн. євро в чотири пілотні проекти, щоб закласти основу для створення європейської мережі центрів експертизи з кібербезпеки, яка допоможе посилити дослідження та координацію кібербезпеки в ЄС. Чотири пілоти, CONCORDIA, ECHO, SPARTA та CyberSec4Europe, мають завдання внести участь у спільну Європейську дорожню карту з питань кібербезпеки та інновацій після 2020 року та європейську стратегію кібербезпеки для промисловості. Крім того, вони допоможуть ЄС у визначенні та тестуванні моделей управління європейською мережею спеціалістів у сфері центрів передової технології в галузі кібербезпеки [4].

За допомогою політичних ініціатив, таких як Європейська мережа національних координаційних центрів з кібербезпеки і новий Європейський центр компетенції в галузі промислової, технологічної та дослідницької компетенції в області кібербезпеки, ЄС намагається створити відповідне нормативно-правове середовище, яке необхідна не тільки для галузі кібербезпеки, а й для підприємців або потенційних інвесторів [4].

Наприклад, Європейський закон про кібербезпеку передбачає створення системи сертифікації кібербезпеки для продуктів і послуг ІКТ. Такий сертифікат надасть відповідальним операторам, постачальникам цифрових продуктів і послуг, включаючи стартапи, конкурентну перевагу. Це дозволить їм бути більш надійними на глобальному рівні. У той же час це підвищить довіру громадян до таких продуктів і послуг, в результаті чого вони будуть купувати більше продуктів і користуватися більш інноваційними послугами [5].

На додаток до цих політичних дій ЄС зробив оперативні дії в області кібербезпеки, такі як створення мережі груп реагування на інциденти комп'ютерної безпеки (CSIRT), організувавши, наприклад, навчання з кібербезпеки.

ЄС також інвестує кошти в підтримку досліджень і інновацій для розробки нових рішень і технологій в області кібербезпеки. До 2020 року ЄС планує проінвестувати близько 1 млрд. євро в проекти з кібербезпеки і цифрової конфіденційності. Майже половина з цього буде в рамках договірного державно-приватного партнерства з кібербезпеки на період 2017-2020 рр. А на період 2021-2027 рр. Європейська комісія запропонувала збільшити інвестиції ЄС в сферу кібербезпеки в рамках нової програми «Цифрова Європа» [3, с. 17].

Кібербезпека – це складна тема для всього світу. Здатність країни витримати кібератаку є дуже важливо складовою для функціонування цифрової економіки та інформаційного суспільства держави. ЄС і в майбутньому буде прикладати зусилля щодо подальшого підвищення потенціалу кібербезпеки, стійкості та інновацій в Європі. Цілком ймовірно, що європейські підприємства і громадяни побачать ще більше політичних ініціатив, запропонованих Європейською комісією в області кібербезпеки в найближчі роки.

Список використаних джерел

1. Владимирова Т. В. Об обеспечении информационной безопасности в условиях кибепространства. *Вопросы безопасности.* 2014. №3. С. 132–157.
2. Кардава Н. В. Киберпространство как новая политическая реальность: вызовы и ответы. *История и современность.* 2018. № 1–2. С. 152–166.
3. Пантин В. И., Кардава Н. В. Кибербезопасность: проблемы формирования единой политики в Европейском Союзе. *Вестник Пермского университета. Политология*. 2018. № 3 . С. 5–18.
4. Кибербезопасность: рекомендации для ЕС. URL://http://www.lawtrend.org/information-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es (дата обращения: 27.09.2019).

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017). URL://http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cy bsec_comm_en.pdf (Last Accessed: 27.

Науковий керівник: **Харченко Ігор Михайлович**, доцент кафедри міжнародних відносин, міжнародної інформації і безпеки, ХНУ ім. В. Н. Каразіна, кандидат технічних наук, старший науковий співробітник.