***Грановський Микола Володимирович**,*
аспірант кафедри політології та філософії,
Харківський регіональний інститут державного управління
Національної академії державного управління при Президентові України,
м. Харків
ORCID 0000-0002-8554-7456

УДК 351.004.7.056.5 (477) (045) **doi: 10.34213/tp.19.04.27**

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАПОБІГАННЯ ТА ПРОТИДІЇ КІБЕРНЕТИЧНИМ ЗАГРОЗАМ – ДОСВІД РЕСПУБЛІКИ ПОЛЬЩА

У сучасному світі спостерігається тенденція до значного зростання кількості кібератак, які стають все більш витонченими і непередбачуваними.
До уваги пропонується стислий аналіз дій, спрямованих на запобігання та протидію кібернетичним загрозам на прикладі Республіки Польща.
Ключові слова: кібербезпека, кібератака, критичні об'єкти інфраструктури держави, інцидент, міжнародне співробітництво у сфері захисту кіберпростору.

Постановка проблеми. Однією з ключових проблем, що постали перед державами світу, є проблема захисту інформації від викликів і загроз у кіберпросторі. Актуальність проблем кібербезпеки сьогодні не викликає жодних сумнівів, оскільки кожна сучасна людина як в Україні, так і за її межами стикається з необхідністю користування інформаційними системами та технологіями від соціальних мереж, розміщення інформації про свої персональні дані в Інтернеті до користування банківськими рахунками, системами e-commerce тощо.

Аналіз останніх досліджень і публікацій. Дослідження питань кібербезпеки як складника інформаційного захисту держави в сучасних умовах знаходиться в фокусі уваги багатьох зарубіжних науковців: С. Морган, А. Клімбург, М. Шмідт, М. Гедекер, М. Лібіцкі, Дж. Най, І. Зубарєв, М. Безкоровайний, П. Ольховська, Я. Гарбіньскі, О. Кроковська. Величезну увагу до цієї проблематики приділяють і українські вчені, зокрема Д. Дубов, М. Ожеван, В. Фурашев, В. Бурячок, В. Бутузов, В. Толубко, О. Довгань, В. Хорошко, С. Толюпа, М. Балюк, В. Дорошко та ін.

Попри велику кількість досліджень у цій сфері питання забезпечення кібербезпеки як невід'ємного елемента системи інформаційної безпеки, тим більше в умовах гібридної війни (яка, на жаль має місце в України), усе ще залишається відкритим.

Оскільки Польща займається вирішенням цієї проблеми системно та на загальнодержавному рівні, привертаючи особливу увагу запобіганню та протидії кіберзагрозам, пропонується ознайомитися з аналізом польського досвіду у вирішення питань у сфері запобігання та протидії кібернетичним загрозам.

Метою цієї статті є аналіз сучасного стану протидії кібератакам у країнах ЄС, зокрема в Республіці Польща (далі – РП). Досвід зазначеної країни може буди корисним для України в контексті забезпечення інформаційної безпеки та систематизації основних шляхів удосконалення системи кібербезпеки нашої держави.

Виклад основного матеріалу дослідження. 1 серпня 2018 р. Президент Польщі підписав Акт про національну систему кібербезпеки (далі – Закон) [3]. Закон реалізує Директиву (ЄС) 2016/1148 Директиви Європейського парламенту та Ради (ЄС) 2016/1148 про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем на території Європейського Союзу (так звана Директива з мережевої та інформаційної безпеки (NIS Directive) (далі – Директива NIS) [2].

Вона зобов'язує держави – члени ЄС гарантувати мінімальний рівень національної здатності до кібербезпеки шляхом створення компетентних органів та єдиних точок контактів з кібербезпеки, створення команд реагування на комп'ютерні інциденти (CSIRT: англ. Computer security incident response team, або "команда реагування на комп'ютерну безпеку") та прийняття національних стратегій кібербезпеки.

Закон набув чинності 28 серпня 2018 р., але для повного упровадження Директиви NIS в РП необхідно було прийняти додаткові постанови Ради Міністрів РП як виконавчі акти, зокрема низку постанов: від 11 серпня 2018 р. "Про перелік ключових послуг та меж значущості руйнівного ефекту інциденту для надання ключових послуг", від 2 жовтня 2018 р. "Щодо масштабів діяльності та режиму роботи Колегії з питань кібербезпеки", від 16 жовтня 2018 р. "Про види документації щодо кібербезпеки інформаційної системи", від 31 жовтня 2018 р. "Щодо порогів визнання інциденту як серйозного, що використовується для надання ключової послуги"[6].

Директива NIS зобов'язує щодо забезпечення кібербезпеки у сферах послуг, які мають вирішальне значення для підтримки критичної соціально-економічної діяльності держави.

До таких секторів належать: енергетика, транспорт, банківська справа, фінансові установи, сектор охорони здоров'я, водопостачання та цифрова інфраструктура. Закон запровадив концепцію системи кібербезпеки, яку спрямовано на забезпечення кібербезпеки та запобігання і протидію кіберзагрозам [4] на національному рівні, включаючи безперебійне надання ключових послуг та цифрових послуг шляхом досягнення відповідного рівня безпеки інформаційних систем, що використовуються для надання цих послуг та забезпечення поводження з інцидентами. Суб'єкти, що складають Національну систему кібербезпеки (НСК):

– ключові оператори;
– провайдери цифрових послуг;
– державні установи;
– компетентні органи влади;
– CSIRT на національному рівні,
– Єдиний контактний пункт з питань кібербезпеки;
– суб'єкти, що надають послуги з кібербезпеки.

Завдяки зазначеному Закону також з'явилися нові поняття: інциденти (критичні, серйозні, значні, у державній структурі), послуги (ключові та цифрові), вразливість чи управління інцидентами.

Інцидент – це подія, що має або може негативно вплинути на кібербезпеку. Закон виділив кілька типів їх. Критичний інцидент – призводить до завдавання шкоди громадській безпеці чи порядку, міжнародним чи економічним інтересам, функціонуванню громадських інститутів, громадянським правам і свободам або здоров'ю чи життю людей. Такі випадки класифі-

куються відповідними CSIRT, про які йдеться нижче. Серйозний інцидент – може спричинити значне зниження якості або перервати безперервність ключової послуги. Значний інцидент – суттєво впливає на надання цифрової послуги. Інцидент у державній структурі – може спричинити зниження якості або переривання публічного завдання, яке здійснює державний орган.

Виникнення інциденту може порушити роботу цифрової послуги – надається в електронному вигляді – та ключової послуги – важливої для підтримки критичної соціальної чи економічної діяльності. Перелік ключових послуг включено в Постанову Ради Міністрів РП від 11 вересня 2018 р. щодо переліку ключових послуг та пороги значущості руйнівного ефекту інциденту для надання ключових послуг.

У зв'язку з новими нормативними актами ключові оператори послуг також відокремлюються (додаток 1 до Закону, перелік послуг від Положення та невіддільність надання послуг з інформаційних систем) та покладають на них зобов'язання, включаючи:

– проведення систематичної оцінки ризиків та управління інцидентами, здійснення відповідних технічних та організаційних заходів, збір інформації про загрози кібербезпеки та вразливості до інцидентів, управління інцидентами та застосування заходів щодо запобігання та обмеження впливу інцидентів на безпеку інформаційних систем;

– розроблення, застосування та оновлення документації щодо кібербезпеки інформаційної системи, що використовується для надання ключової послуги та встановлення нагляду за цією документацією;

– створення внутрішніх структур, відповідальних за кібербезпеку, або укладення договору з суб'єктом господарювання, що надає послуги з кібербезпеки;

– забезпечення проведення аудиту безпеки інформаційної системи щонайменше раз на два роки.

У разі виникнення інциденту відповідно до Закону має відбутися здійснення його обслуговування. Мається на увазі діяльність з виявлення, запису, аналізу, класифікації, визначення пріоритетів, вжиття коригувальних дій та обмеження наслідків інциденту. Закон окреслив три органи на національному рівні, які займаються реагуванням на комп'ютерні інциденти та управління ними. Відповідно до термінології, прийнятої в Директиві NIS 2016/1148, вони мають назву CSIRT. У Польщі це CSIRT GOV, CSIRT MON, CSIRT NASK.

CSIRT GOV – урядова команда реагування на комп'ютерні випадки на чолі з Головою Агенції внутрішньої безпеки – завданням її є розроблення та координація розгляду інцидентів, про які повідомляють найважливіші суб'єкти державного сектору в секторі державних фінансів, підрозділи, які звітують та контролюються прем'єр-міністром (включаючи RCB (урядовий центр безпеки), KNF (комісія фінансового контролю), UZP (управління державних замовлень), URE (управління енергетичного регулювання), PGRP (генеральна прокуратура РП), Національний банк Польщі, Банк Національного Господарства (Bank Gospodarstwa Krajowego) та суб'єкти, щодо яких розповсюджується Закон про управління кризовими ситуаціями, тобто суб'єкти, системи інформаційно-комунікаційних технологій (ІКТ) чи мережі ІКТ, включені до єдиного переліку об'єктів, інсталяцій, пристроїв та послуг, що входять до критичної інфраструктури ,

CSIRT MON – система реагування на комп'ютерні випадки Міністерства національної оборони РП. Вказана структура координує розгляд інцидентів, про які повідомляють суб'єкти, підпорядковані міністру національної оборони або під наглядом їх, та підприємці, які мають особливе економічне та оборонне значення.

Управління NASK CSIRT здійснюється Науково-академічною комп'ютерною мережею та реагує на інциденти, про які інформують науково-дослідні інститути, Польське агентство аеронавігаційних служб (Polska Agencja Żeglugi Powietrznej) або фізичні особи.

CSIRT забезпечують цілісну і повну систему управління ризиками на національному рівні, виконуючи завдання щодо протидії загрозам кібербезпеки міжсекторного та транскордонного характеру – вони знаходяться в європейській мережі CSIRT та надають інформацію про інциденти іншим державам та іншим контактним точкам. Команди виконують ці завдання, співпрацюючи між собою, з органами, компетентними з питань кібербезпеки, міністром, що відповідає за питання IT та проксі. Вони контролюють загрози та інциденти в кібербезпеці на національному рівні та оцінюють пов'язаний з ними ризик. Вони також можуть видавати повідомлення про виявлені загрози.

CSIRT зобов'язані інформувати один одного та урядовий центр безпеки про критичний інцидент, який може спричинити кризову ситуацію щодо безпеки чи громадського порядку. Команди спільно розробляють основні елементи процедур поводження з інцидентом, у якому вони співпрацюють між собою.

Закон також запроваджує поняття галузевої групи з кібербезпеки, тобто команди, створеної органом, компетентним у визначеному секторі чи підгалузі. Ця команда відповідає за оброблення або підтримку поводження з інцидентами у своєму секторі чи підсекторі.

Іншим органом, створеним новим законом, є Група з критичних інцидентів, яка відіграє допоміжну роль у вирішенні критичних випадків, про які повідомляє мережа CSIRT. Команда складається з представників урядового центру безпеки, а також CSIRT MON, CSIRT NASK та керівника Агенції внутрішньої безпеки. Його очолює директор урядового центру безпеки.

Відповідно до Європейської директиви було створено Єдиний контактний пункт, який підпорядковується Міністерству оцифрування та відповідає:

– за створення правової бази для функціонування зони кібербезпеки Республіки Польща, включаючи забезпечення узгодженості;

– виконання функції зв'язку для забезпечення співпраці з суб'єктами, відповідальними за кібербезпеку;

– збирання та обробляння отриманої інформації, серед іншого ключові оператори послуг;

– контроль за дотриманням організаційних і технічних вимог суб'єктами, що надають послуги з кібербезпеки;

– пересилання на прохання відповідної CSIRT повідомлення про великий інцидент або значний інцидент за участю двох або більше держав – членів Європейського Союзу до єдиних точок контактів інших держав – членів ЄС;

– забезпечення участі представника Республіки Польща у Групі співпраці;

– забезпечення співпраці з Європейською Комісією у сфері кібербезпеки;

– координація співпраці між органами, компетентними з питань кібербезпеки Республіки Польща, з відповідними органами держав – членів ЄС;

– співпраця з іншими органами, наприклад правоохоронними органами та компетентним органом із питань захисту даних [5].

Суб'єктом, відповідальним за координацію діяльності та реалізацію політики уряду щодо забезпечення кібербезпеки в Республіці Польща, є Урядовий уповноважений з питань кібербезпеки (його функції виконує Державний секретар Міністерства оцифрування РП К. Оконьський). До основних завдань Урядового уповноваженого належать, зокрема, аналіз та оцінка функціонування національної системи кібербезпеки, контроль за процесом управління ризиками національної системи кібербезпеки, надання висновків щодо проектів нормативно-правових актів та інших урядових документів, що впливають на виконання завдань з кібербезпеки, видання рекомендацій та ініціювання національних вправи з кібербезпеки. Повноважний представник повинен до 31 березня щороку подавати на розгляд Ради Міністрів звіт за попередній календарний рік, включаючи інформацію про поточну діяльність у сфері кібербезпеки в країні. При Раді Міністрів створено Колегію кібербезпеки. Це дорадчий та консультативний орган з питань планування, нагляду та координації діяльності CSIRT, галузевих груп з питань кібербезпеки та компетентних органів. Створення Колегії було спрямовано на підтримку більшої системної узгодженості та прозорості, надання питанням кібербезпеки відповідного рангу, а також забезпечення формулювання послідовних вказівок та планів протидії загрозам кібербезпеці. Розроблення та прийняття Стратегії кібербезпеки накладається положеннями Закону від 5 липня 2018 р. (розділ 13). Тоді як ст. 90 встановлює граничний термін реалізації Стратегії резолюцією до 31 жовтня 2019 р. Документ визначає стратегічні цілі та відповідні політичні заходи, спрямовані на досягнення та підтримку високого рівня кібербезпеки в Республіці Польща. Виникла потреба в оцінці та перегляді поточного стратегічного документа на 2019 р., тобто Національної рамки політики кібербезпеки Республіки Польща на 2017–2022 рр., прийнятої Постановою № 52/2017 Ради Міністрів від 27 квітня 2017 р., та відповідного Плану дій на реалізацію Національної рамки політики кібербезпеки Республіки Польща на 2017–2022 рр. Постійно змінюються умови, пов'язані з безпекою, особливо в кіберпросторі, вимагають швидкої та рішучої реакції державних органів. За інформацією Канцелярії прем'єр-міністра: проект резолюції спрямовано на створення стратегії кібербезпеки. Стратегія має політичний та стратегічний характер, тоді як на операційному рівні її реалізація забезпечить детальний план дій. План дій описує суб'єктів, які беруть участь у реалізації Стратегії, та заходів щодо її реалізації. Під час розроблення Стратегії було використано передовий досвід та рішення, запропоновані Міжнародним союзом зв'язку, та досвід інших країн [1].

У 2018 р. Вища контрольна палата (NajwyższaIzba Kontroli) здійснила аудит у сфері управління інформаційною безпекою в підрозділах місцевого самоврядування. Результати аудиту показали недостатню обізнаність осіб, які виконують функції органу НСК, щодо важливості інформаційної безпеки. Також було виявлено недостатнє фінансове забезпечення для реалізації необхідних проектів та недостатню чисельність фахівців у галузі інформаційної безпеки.

Діяльність Міністерства оцифрування Республіки Польща. Метою Закону про національну систему кібербезпеки, підготовленого Міністерством оцифрування РП (Ministerstwo Cyfryzacji RP), було розроблення законодавчих норм, що дозволять реалізувати Директиву NIS та створити ефективну систему безпеки ІКТ на національному рівні. З метою реалізації зазначених нормативних актів Урядовий уповноважений взаємодіє з різними профільними структурами, наприклад:

– з компетентними органами у галузі підготовки кадрів;

– з CSIRT щодо керівних принципів;

– з органами місцевого самоврядування;

– у галузі навчання та електронного навчання;

– з технологічними партнерами в галузі обміну інформацією про нові загрози та технології.

Науково-академічна комп'ютерна мережа – Національний науково-дослідний інститут (Naukowa i AkademickaSiećKomputerowa – Państwowy Instytut Badawczy (NASK) – доручала проводити заходи з підвищення рівня обізнаності у сфері кіберзагроз серед працівників державної адміністрації. Передбачається реалізація двох завдань:

1. Побудова платформи для електронного навчання (e-CTP – Cyber Training Platform) для працівників державного управління, включаючи органи місцевого самоврядування.

Випробування на платформі мають відбутися до кінця поточного року в офісах органів державної влади, а платформу буде запущено в повному обсязі у 2020 р. Офіси будуть запрошені послідовно використовувати електронне навчання відповідно до встановленого графіку. Планується, що платформа буде доступна тимчасово для конкретної державної адміністрації та протягом цього час не буде доступною для інших. Також було прийнято рішення щодо створення кол-центру, який підтримуватиме згадану платформу.

2. Проведення спеціалізованих тренінгів у регіонах для представників окремих структурних підрозділів органів державної влади та місцевого самоврядування в рамках Закону про Національну систему кібербезпеки (НСК).

Мета тренінгів – підвищити рівень безпеки в органах державного управління та органах місцевого самоврядування шляхом підвищення рівня обізнаності та розбудови компетентності у сфері кібербезпеки. Передбачається організація чотирьох інформаційних зустрічей (організовані на базі чотирьох обраних/готових до співпраці місцевих державних адміністрацій), які охоплюватимуть загалом близько чотирьох сотень державних службовців на рівні регіону, відповідальних за кібербезпеку. Кінцевий термін реалізації: вересень – грудень 2019 р. Подальші офіси мають приєднатися до стаціонарного навчання у 2020 р. Обидва проектні завдання підтримуватимуться трьома командами NASK: Академія NASK, IT School та NASK CSIRT. Координацію забезпечуватиме відділ кібербезпеки Міністерства оцифрування.

Наступним аспектом діяльності, що розвивається НСК, є технологічне співробітництво. Це особливо важливо через двосторонні угоди з технологічними партнерами та обмін інформацією (вразливість, загрози, інструменти моніторингу кібербезпеки). Однак це ще не всі зусилля для створення потужної системи кібербезпеки в Польщі.

У рамках дослідного проекту було створено Національну цифрову платформу, яка передбачає створення прототипу комплексної, інтегрованої сис-

теми моніторингу, зображень та попереджень щодо загроз кіберпростору держави, оцінки потенційних наслідків та скоординованого реагування на комп'ютерні інциденти на національному рівні. За допомогою цього проекту Міністр оцифрування забезпечує розвиток або підтримку системи ІКТ, яка підтримує:

– обмін інформацією з метою співпраці між суб'єктами, що входять до національної системи кібербезпеки;

– формування та прийняття рекомендацій щодо дій, що підвищують рівень кібербезпеки;

– звітування та поводження з інцидентами, оцінка ризиків на національному рівні;

– попередження про загрози кібербезпеці.

Крім того, NASK розробляє посібники, які висвітлюють тему організації НСК, правила звітності про випадки та захист персональних даних. Вони також публікуються на веб-сайтах МС, а мета їх – широко розповсюджувати знання та формувати компетенції.

Ще одна ініціатива – "Партнерство заради кібербезпеки" – інструмент добровільної співпраці та обміну досвідом та інформацією про загрози та інциденти в кібербезпеці. Основним інструментом партнерства є: обмін інформацією у сфері кібербезпеки, про інциденти та значні загрози, що виходять (за інформацією Партнера) за межі внутрішніх подій, забезпечення відповідного реагування та провадження у вирішенні проблем. У рамках участі в програмі учасники можуть:

– передавати інформацію про інциденти NASK;

– повідомити координатора програми (NASK) про загрози, що спостерігаються;

– ділитися знаннями в галузі кібербезпеки;

– ініціювати створення цільової групи.

У рамках програми, яка наразі складається з понад півсотні тристоронніх угод, було підписано сім угод з органами місцевого самоврядування на рівні воєводства (місцевої державної адміністрації).

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. Забезпечення кібербезпеки в Польщі та побудова її стійкої системи є безперервним процесом. Варто зазначити, що він стає більш усвідомленим та спланованим, незважаючи на виклики та труднощі, які виникають. Окрім тих, що вказані після аудиту Вищої контрольної палати (ВКП), можна також говорити про відсутність достатньої кількості експертів на ринку, труднощі в гармонізації нормативно-правових актів, що стосуються різноманітності секторів, різних тлумачень закону та встановлених вимог. Тим не менш реалізація Стратегії восени цього року та дії Міністерства оцифрування можуть прискорити розроблення відповідних механізмів забезпечення кібербезпеки в РП.

Забезпечення кібербезпеки в Європі, зокрема у Польщі, та побудова ефективної системи протидії кіберзагрозам є тривалим і системним процесом, до якого необхідно долучитися й Україні як повноправному партнеру.

Враховуючи польський досвід та досвід міжнародних партнерів, пропонується опрацювати питання щодо вдосконалення системи роботи чинних структур в Україні, які опікуються інформаційною безпекою, а також розглянути можливість створення додаткових профільних структур (у разі

необхідності) на рівні центральних органів виконавчої влади, а також цільових груп на базі новостворених відомств та науково-дослідних установ для подальшої роботи в напрямі запобігання та протидії кіберзагрозам у державному управлінні; дигіталізації та розвитку галузі електронних комунікацій; визначення перспективної організаційно-технічної моделі кіберзахисту та удосконалення освіти у сфері кібербезпеки тощо.

За сучасних умов інформаційний складник набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки країни.

Список використаних джерел

1. Biuletyn informacji publicznej Kancelarii Prezesa Rady Mibistrów RP. URL:https://bip.kprm.gov.pl/kpr/wykaz/r953654207552,Projekt-uchwaly-Rady-Ministrow-w-sprawie-Strategii-Cyberbezpieczenstwa-Rzeczypos.html.

2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. URL: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL

3. Dziennik Ustaw RP 2018 rok. URL: http://www.dziennikustaw.gov.pl/du/2018.

4. Encyklopedia Zarządzania. URL: https://mfiles.pl/pl/index.php/Cyberbezpieczeństwo.

5. Strona internetowa Ministerstwa Cyfryzacji RP. URL: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa.

6. Ustawa z 5 lipca 2018 r. "O krajowym systemie cyberbezpieczeństwa". URL: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf.

References

1. Biuletyn informacji publicznej Kancelarii Prezesa Rady Mibistrów RP. URL:https://bip.kprm.gov.pl/kpr/wykaz/r953654207552,Projekt-uchwaly-Rady-Ministrow-w-sprawie-Strategii-Cyberbezpieczenstwa-Rzeczypos.html.

2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. URL: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL

3. Dziennik Ustaw RP 2018 rok. URL: http://www.dziennikustaw.gov.pl/du/2018.

4. Encyklopedia Zarządzania. URL: https://mfiles.pl/pl/index.php/Cyberbezpieczeństwo.

5. Strona internetowa Ministerstwa Cyfryzacji RP. URL: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa.

6. Ustawa z 5 lipca 2018 r. "O krajowym systemie cyberbezpieczeństwa". URL: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf.

Hranovskyi M. V., *Postgraduate Student of Political Science and Philosophy Department,*
KRI NAPA, Kharkiv
ORCID 0000-0002-8554-7456

STATE POLICY IN THE FIELD OF PREVENTION AND COUNTERACTION TO CYBERTHREATS – EXPERIENCE OF THE REPUBLIC OF POLAND

In today's world there is a tendency for a significant increase in the number of cyber threats and attacks that are becoming more sophisticated and unpredictable.

Ensuring cybersecurity is extremely important for Ukraine in conditions of a hybrid war. The Law of Ukraine on Cybersecurity and further development of international cooperation in the field of cyberspace protection with the United States and the European Union is more urgent than ever. It is necessary to improve international mechanisms and a common international policy to develop and implement effective methods for combating cyber threats.

For attention offers a concise analysis of actions aimed at preventing and counteracting cyber threats through the example of the Republic of Poland.

Ensuring cybersecurity in Europe, in particular in Poland, and building a sustainable cyber-threat system –is a continuous process and a long-standing process that needs to be joined by Ukraine as a full partner.

Considering the Polish experience and the experience of international partners, it is proposed to address the issues of improving the system of work of the existing information security structures in Ukraine, as well as to consider the creation of additional profile structures at the level of central executive authorities, as well as target groups based on newly created agencies and scientific and research institutions for further work in the field of cybersecurity and improvement of public administration; digitalization and development of the electronic communications industry; definition of a promising organizational and technical model of cyber defense and improvement of cybersecurity education, etc.

In today's context, the information component is gaining more weight and becoming one of the most important elements of national security.

Key words: cybersecurity, cyber attack, critical objects of state infrastructure, international cooperation in the field of cyberspace protection.

Надійшла до редколегії 07.11.2019 р.