ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference "Cybersecurity in Ukraine: Legal and Organizational Issues"

Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року

ОДУВС
м. Одеса
2022

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference "Cybersecurity in Ukraine: Legal and Organizational Issues"

Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року

Одеса
ОДУВС
2022

Рекомендовано до друку рішенням кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання:
К38 матеріали міжн. наук. практ. конф., м. Одеса, 23 листопада 2022 р. Одеса : ОДУВС, 2022. 152 с.
ISBN 678-717-70204

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 23 листопада 2022 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), здобувачам вищої освіти першого та другого півня освіти.

РОЗВИТОК КІБЕРЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР ДЕРЖАВ – НАГАЛЬНА ПРОБЛЕМА СУЧАСНОСТІ

Володимир ПЯДИШЕВ
професор кафедри кібербезпеки та
інформаційного забезпечення ОДУВС
д.ю.н., доцент

Новий час призвів до нового ставлення до захисту критичних інфраструктур держав. Одним з прикладів розуміння світовою спільнотою необхідності змін ставлення стало проведення Онлайн-тренінгу «Protection of public spaces, critical infrastructures and cybersecurity» Європейським поліційним коледжем (CEPOL) — агентством Європейського Союзу, яке об'єднує старших офіцерів національних поліцій ЄС з метою підготовки до боротьби з транскордонною злочинністю, забезпечення громадської безпеки і правопорядку [1].

Зазначений Онлайн-тренінг тривав два тижні: з 17 по 28 жовтня 2022 року. Тематика тренінгу: «Захист публічних просторів, критичної інфраструктури та кібербезпека», – відбивала розвиток такої небезпечної тенденції сучасності як атаки на критичні інфраструктури.

Навчальні матеріали для тренінгу було надано відомими міжнародними правоохоронними агентствами:

- ENISA – Агентство Європейського Союзу з кібербезпеки [2];
- Головне управління мереж зв'язку, контенту та технологій Євросоюзу;
- Європейський контртерористичний центр, ЄВРОПОЛ [3];
- Об'єднаний дослідницький центр Єврокомісії;
- Управління ООН по боротьбі з тероризмом;
- Центр безпеки та кризових ситуацій, Європейський єврейський конгрес,

а також відомими правоохоронними агентствами держав: Нідерланди, Іспанія, Бельгія, Португалія, Румунія.

Протягом тренінгу багато часу було приділено захисту критичних інфраструктур від **фізичних атак**. Було розглянуто наступні питання:

- ✓ захист критичної інфраструктури;
- ✓ оцінка ризиків і заходи безпеки на критичних інфраструктурах;
- ✓ здійснення підходу до управління ризиками критичної інфраструктури;
- ✓ захист критичної інфраструктури в контексті **гібридних** загроз;
- ✓ захист критичної інфраструктури від терористичних атак;
- ✓ цілі тероризму: розвиток загроз;
- ✓ критичні об'єкти та громадські простори. Відмінності та подібності;
- ✓ захист громадських просторів;
- ✓ внутрішні загрози;
- ✓ Проект Об'єднаного дослідницького центру Єврокомісії щодо дронів

Певної уваги було приділено й розгляду питань, що пов'язані з **кібератаками** на критичні інфраструктури:

- ✓ критична цифрова інфраструктура;
- ✓ безпека та захист кіберсистем;
- ✓ роль центру безпеки та кризових ситуацій у захисті громадських місць та кібербезпеці;
- ✓ стратегія кібербезпеки ЄС.

Проте всі наведені протягом зазначеного Онлайн-тренінгу приклади з атаками на критичні інфраструктури держав Європи не йдуть у жодне порівняння з тими атаками, що здійснюються сьогодні Російською федерацією проти України. Отже представникам України довелося ознайомити учасників Онлайн-тренінгу, представників правоохоронних органів Євросоюзу з масштабами та глибиною як фізичних, так кібератак на критичні інфраструктури України. Зазначене справило на закордонних колег глибоке гнітюче враження. Всі вони висловили підтримку Україні та особисту готовність допомагати.

Глибокому аналізу **кібератак** на критичні інфраструктури України була присвячена інша подія, Міжнародна конференції «Кібербезека критичних інфраструктур під час війни», яка відбулася 14.11.2022. Конференція проводилася під егідою Ради національної безпеки і оборони України та Національного координаційного центру з кібербезпеки. У конференції взяли участь більше 100 учасників. Спікерами на конференції були:

- Сергій Прокопенко, Голова Національного координаційного центру України, РНБО
- Ірина Тимошенко, Голова Служби захисту критичної інфраструктури, РНБО
- Клаудія Іаннаццо, Головний виконавець Catalisto (міжнародної організації, що створює екосистеми для вирішення найскладніших у світі викликів кібербезпеки)

- Владлен Басистий, Старший керівник Проекту з кібербезпеки CRDF Global (Фонд цивільних досліджень та розвитку США) [4].

У своїй першій доповіді Старший керівник Проекту з кібербезпеки Фонду цивільних досліджень та розвитку США, пан Владлен Басистий підкреслив такі моменти:

- хронологія кібератак на Україну після Революції Гідності;
- сучасні тенденції протягом вересня – листопада;
- розвиток Національної системи кібкербезпеки;
- партнерство з громадою;
- підтримка України з боку світової спільноти;
- пріоритети.

Від РНБО Голова Служби захисту критичної інфраструктури, пані Ірина Тимошенко присвятила свою доповідь таким питанням:

- Закон України «Про критичну інфраструктуру», що набув чинності 16.11.2021 і введено в дію 15.06.2022
- Національна система захисту критичної інфраструктури;
- Закон України «Про режим воєнного стану»№
- Закон України «Про поправку до деяких законів України через створення та впровадження Державної політики у сфері захисту критичної інфраструктури», що має набути чинності 05.12.2022;
- Роль Державної служби спеціального зв'язку та захисту інформації в Україні;
- Статистика збитків, що понесла Україна через атаки та її критичну інфраструктуру;
- Обладнання, що потрібне для відновлення критичної інфраструктури у секторі палива та енергетики;
- Проблемі питання у сфері засобів зв'язку;
- Потреби у навчанні фахівців для сфери захисту критичної інфраструктури.

Головний виконавець Catalisto (міжнародної організації, що створює екосистеми для вирішення найскладніших у світі викликів кібербезпеки), пані Клаудія Іаннаццо у своїй доповіді «Еволюція кіберзагроз у Східній Європі» звернула увагу на:

- ключові ідеї;
- перспективи організації CALISTO;
- тенденції кібератак у Європі з січня 2021;
- головних акторів кібератак;
- взаємодію організації та її роль акселератора в організації захисту критичних інфраструктур.

У своїй другій доповіді Старший керівник Проекту з кібербезпеки Фонду цивільних досліджень та розвитку США, пан Владлен Басистийзвернув увагу на:

- збитки критичній інфраструктурі України з лютого 2022;

- партнерство державного та приватного секторів у захисті критичної інфраструктури в Україні з лютого 2022;
- на планах політики України щодо захисту критичної інфраструктури, правової бази та рамкового розвитку;
- на напрямах впровадження передових практик у цій сфері;
- на діяльності CRDF Global України у 2021 році;
- на спільній діяльності CRDF Global та РНБО з 24.02.2022.

Зокрема було вказано:

- CRDF developed and presented to CIP Flobal grogram proposal for CIP system development in Ukraine
- started preparation for the implementation of the first phase of CIP program
- CRDF розробив і представив CIP глобальну програмну пропозицію щодо розвитку системи CIP в Україні
- розпочато підготовку до впровадження першої фази Програми захисту критичних інфраструктур

У процесі запитів та відповідей встановлено необхідність створення навчального напряму: «Підготовка фахівців для захисту критичної інфраструктури від кібератак».

ВИСНОВКИ:

1. Сьогодні Україна більш, ніж інші держави потребує зміцнення захисту критичних інфраструктур від кібератак.
2. Для цього необхідні матеріальні ресурси, навчальні матеріали, технічна база та підготовлені фахівці.
3. Необхідно розпочати здійснювати освіту за навчальним напрямом: «Підготовка фахівців для захисту критичної інфраструктури від кібератак».

Література:

1. Making Europe a safer place through law enforcement training and learning, Site. URL: https://www.cepol.europa.eu/ (дата звернення 15.11.2022).
2. ENISA – European Union Agency for Cybersrcurity. *An official website of the European Union*, Site. URL: https://www.enisa.europa.eu/(дата звернення 15.11.2022).
3. About Europol. Helping make Europe safer. Site. URL: https://www.europol.europa.eu/about-europol (дата звернення 15.11.2022).
4. CRDF Global Helps Ukraine Protect Critical Infrastructure. Site. URL: https://www.crdfglobal.org/news/crdf-global-helps-ukraine-protect-critical-infrastructure/ (дата звернення 15.11.2022).

ЗМІСТ