КІБЕРБЕЗПЕКА

ЗАГАЛЬНИЙ ОГЛЯД

Сьогодні, коли Україна захищає свою безпеку, незалежність і демократію від агресії з боку Росії, кіберпростір – це життєво важливий фронт. За останні роки USAID вклало значні ресурси у зміцнення спроможності України протистояти кібератакам і ліквідовувати їхні наслідки; ці атаки, джерелом яких є Росія, спрямовуються проти Уряду України та підприємств критичної інфраструктури. USAID допомагає Україні підвищувати рівень кібербезпеки у рамках загальних заходів, що мають сприяти економічному зростанню та розвитку демократичного врядування у країні. Ця підтримка сприяє розбудові належного потенціалу міністерств і відомств Уряду та комітетів Верховної Ради України, забезпеченню демократичного виборчого процесу, а також кращому розумінню того, наскільки важливою є кібербезпека, серед громадянського суспільства, бізнесу та широкого загалу. Від початку повномасштабного вторгнення Росії у лютому 2022 р., ми розширили програми допомоги у цій сфері, аби сприяти більш ефективній протидії кібератакам на мережі публічних комунікацій та відновленню діяльності інформаційних систем після таких нападів, а також забезпеченню безперебійного голосового зв'язку та передачі даних.

ЗАВДАННЯ ДОПОМОГИ

Забезпечити кращу спроможність України до запобігання кібератакам, реагування на них і пом’якшення їхніх наслідків, а також до швидкого відновлення та забезпечення подальшої діяльності критично важливої інфраструктури.

НАШІ ПРОГРАМИ

ПРОЕКТ «КІБЕРБЕЗПЕКА КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ»
Розрахований на чотири роки проект USAID «Кібербезпека критично важливої інфраструктури в Україні» має вартість 38 млн. дол. США та розпочав свою діяльність у травні 2020 р. Його завдання – підвищити рівень готовності критично важливої інфраструктури до кібератак та сприяти її кращому захисту за рахунок допомоги, яка надається за трьома основними напрямами: 1) зміцнення середовища, що є сприятливим для кібербезпеки; 2) формування кадрового потенціалу України у сфері кібербезпеки; 3) створення стійкої кібербезпекової індустрії. Діяльність проекту спрямована на підвищення якості продуктів і послуг у сфері кібербезпеки на основі ширшої співпраці державних

установ і приватного бізнесу; ще одним його завданням є розширення ринкових можливостей для українських компаній, які спеціалізуються на питаннях кібербезпеки – шляхом забезпечення доступу до капіталу, а також до нових внутрішніх і зовнішніх ринків. Одним із потужних елементів проекту є розбудова стійкості української енергетики до кібератак. Електроенергетичні підприємства, які співпрацюють з проектом, розробляють п'яти- та десятирічні плани розвитку мереж, а їхні спеціалісти проходять навчання з питань удосконалення організаційної структури, виробничої діяльності та здійснення закупівель. Підприємства також виробляють стратегічні підходи до вирішення питань кібербезпеки в енергетиці та беруть участь у навчальних заходах щодо модернізації мереж розподілу та постачання електрики, завдяки чому вони мають стати стійкішими до кібератак. Ще одним напрямом роботи проекту є сприяння діалогу між підприємствами та регуляторами галузі, аби забезпечити фінансову доцільність заходів з модернізації мереж з метою їхнього захисту від кібератак.

Після повномасштабного вторгнення Росії, у рамках проекту було профінансовано діяльність технічних спеціалістів, які забезпечили практичну допомогу основним надавачам послуг державного сектору (у т.ч. міністерствам і підприємствам критично важливої інфраструктури) з метою виявлення шкідливого програмного забезпечення та відновлення роботи систем після надзвичайних ситуацій у сфері кібербезпеки. Ці заходи є продовженням тривалої допомоги з боку USAID підприємствам-надавачам основних послуг на рівні регіонів, передусім в енергетичному секторі.

Окрім того, під час вторгнення Росії USAID надало цим підприємствам, посадовцям органів влади та персоналу об'єктів критично важливої інфраструктури у сфері енергетики та телекомунікацій 6750 приладів екстреного зв'язку – у т.ч. супутникові телефони та термінали передачі даних.

Програма «Відповідальне та підзвітне врядування в Україні»

У 2016 році USAID розпочало програму «Відповідальне та підзвітне врядування в Україні». Ця програма, яка розрахована на 9 років і має вартість 81 млн. дол. США, покликана сприяти розбудові в Україні виборчих і політичних процесів, у центрі уваги яких перебувають інтереси громадян. Напрям діяльності програми у сфері кібербезпеки передбачає співпрацю USAID з Центральною виборчою комісією (ЦВК), аби сприяти розвитку її потенціалу та протидіяти кіберзагрозам для виборчих систем, які дедалі зростають. У рамках програми також було проведено оцінку стану інформаційного забезпечення ЦВК; спільно з основними зацікавленими сторонами у сферах виборів і кібербезпеки, здійснювалися критично важливі кроки з підвищення кібербезпеки виборчої інфраструктури, проводились навчальні заходи з кібергігієни для членів виборчих комісій усіх рівнів, представників громадянського суспільства, політичних партій і парламенту. У 2019 році участь у цьому навчанні взяли загалом 642 особи. Ще одним напрямом діяльності програми були розробка та впровадження курсів навчання з питань кібербезпеки для фахівців IT-сектору України та інших країн. Програма забезпечила зміцнення кіберстійкості систем, які використовуються для підрахунку результатів виборів, а також реєстру виборців, та допомогла ЦВК протистояти кібератакам під час виборів Президента України (2019 р.) та позачергових парламентських виборів. Це сприяє підтриманню громадської довіри до виборчого процесу.

ПРОГРАМИ ШТАБ-КВАРТИРИ USAID У ВАШИНГТОНІ ТА РЕГІОНАЛЬНІ ПРОЕКТИ

РЕГІОНАЛЬНА ПРОГРАМА ЗІ ЗМІЦНЕННЯ КІБЕРБЕЗПЕКИ В ЕНЕРГЕТИЦІ

Енергетична асоціація США та Національна асоціація членів комісій з регулювання комунальних підприємств США спільно забезпечують допомогу енергетичному сектору України у підвищенні рівня кібербезпеки. Ця регіональна програма вартістю 1 млн. дол., участь у якій також беруть Молдова, Вірменія та Грузія, створює механізми обміну знаннями та найкращим досвідом серед усіх структур енергосектору у цьому регіоні. Її заходи спрямовані на зміцнення кібербезпекового потенціалу регуляторів енергетичного сектору та підприємств із передачі та розподілу електроенергії.