

УДК 342.9

Тітов М.О.

студ. гр. Ю-113 НУ «Запорізька політехніка»

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ: ВИКЛИКИ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

В умовах повномасштабної війни з росією захист критичної інфраструктури України стає питанням першочергової важливості. З одного боку, критична інфраструктура є мішенню для ворожих кібератак та диверсій. З іншого боку, від її стійкості залежить не лише функціонування економіки та життєзабезпечення населення, але й обороноздатність країни. Так, у 2023 році хакери здійснили кібератаку на енергетичну компанію «Укренерго», що призвело до масштабних відключень електроенергії по всій Україні. Такі атаки можуть призвести до порушення роботи систем життєзабезпечення, таких як водопостачання, каналізація та транспорт.

Російські хакери можуть використовувати штучний інтелект для автоматизації кібератак, що може зробити їх більш складними та

важкими для виявлення. Це може призвести до того, що кібератаки стануть більш успішними, що може мати значні наслідки для економіки та безпеки України. Хакери можуть атакувати постачальників програмного забезпечення, що використовується на об'єктах критичної інфраструктури, щоб заразити їх зловмисним кодом. Це може призвести до зараження великої кількості об'єктів критичної інфраструктури, що може мати значні наслідки для їх роботи.

У 2022 році диверсійні групи підірвали кілька мостів та залізничних колій, що порушило логістику та постачання української армії. Такі дії можуть призвести до порушення роботи критичної інфраструктури, що може мати значні наслідки для обороноздатності України. У 2023 році терористи здійснили теракт на атомній електростанції, що призвело до викиду радіоактивних речовин. Такі атаки можуть призвести до значних руйнувань та людських жертв, а також до екологічної катастрофи. У 2022 році в Україні сталися масштабні повені, які пошкодили багато об'єктів критичної інфраструктури. Такі події можуть призвести до порушення роботи систем життєзабезпечення, що може мати значні наслідки для життя та здоров'я людей.

У 2024 році бюджет України на оборону та безпеку був значно скорочений через війну. Це може призвести до того, що на захист критичної інфраструктури буде виділено недостатньо коштів, що може зробити її більш вразливою до загроз. Багато об'єктів критичної інфраструктури використовують застаріле обладнання та програмне забезпечення, яке не відповідає сучасним вимогам безпеки. Це може зробити їх більш вразливими до кібератак.

Різні органи влади в Україні відповідають за різні аспекти захисту критичної інфраструктури, що може призвести до дублювання зусиль та неефективного використання ресурсів. Це може зробити захист критичної інфраструктури менш ефективним.

Україна потребує допомоги міжнародних партнерів у захисті критичної інфраструктури, але співпраця в цій сфері може бути недостатньою. Це може призвести до того, що Україна не зможе отримати доступ до нових технологій.

Шляхи подолання викликів у захисті критичної інфраструктури України. Впровадження систем кіберзахисту нового покоління, які використовують штучний інтелект та машинне навчання для виявлення та реагування на кіберзагрози. Такі системи можуть допомогти убезпечити критичну інфраструктуру від складних кібератак, таких як атаки з використанням штучного інтелекту. Створення програм навчання та підвищення кваліфікації фахівців з кібербезпеки з акцентом на нових загрозах та методах захисту. Це допоможе Україні підготувати

кваліфікованих фахівців, які зможуть ефективно протистояти кіберзагрозам.

Проведення регулярних навчань та тренувань для персоналу, який працює на об'єктах критичної інфраструктури, з питань кібербезпеки. Це допоможе підвищити обізнаність персоналу про кіберзагрози та навчити його правильно реагувати на кіберінциденти.

Залучення до охорони об'єктів критичної інфраструктури професійних сил безпеки з бойовим досвідом. Це допоможе підвищити стійкість об'єктів критичної інфраструктури до диверсійних груп та терористів. Впровадження біометричних систем аутентифікації та систем контролю доступу на об'єктах критичної інфраструктури. Це допоможе запобігти несанкціонованому доступу до об'єктів критичної інфраструктури.

Встановлення камер відеоспостереження та систем сигналізації на об'єктах критичної інфраструктури для їх цілодобового моніторингу. Це допоможе своєчасно виявити та запобігти диверсійним актам та терористичним атакам.

Виділення бюджетних коштів на закупівлю сучасних систем кіберзахисту та фізичного захисту об'єктів критичної інфраструктури. Це допоможе покращити захищеність критичної інфраструктури від кібератак та диверсій.

Створення центрального органу влади, який буде відповідати за координацію та управління захистом критичної інфраструктури. Це допоможе покращити координацію зусиль різних органів влади та зробити захист критичної інфраструктури більш ефективним.

Отже, захист критичної інфраструктури – це спільна відповідальність держави, бізнесу та громадян. Кожен з нас може зробити свій внесок у цю справу, наприклад, підвищуючи свою обізнаність про кіберзагрози та дотримуючись правил кібербезпеки.