

**КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ**

Кожна країна визначає свої власні найважливіші інформаційні інфраструктури. Зростаюча технологічна взаємозалежність базується на складній мережі компонентів, тому важливим завданням Збройних Сил України є організація належного захисту державної таємниці.

В наш час інформаційні інфраструктури піддаються все більш численним і різноманітним загрозам і чинникам уразливості, які створюють загрозу для державної таємниці. Захист найважливіших інфраструктур включає, зокрема, виявлення загроз і зменшення вразливості найважливіших інформаційних інфраструктур, мінімізацію збитку і часу на відновлення у разі пошкодження або спроб порушення захисту, а також виявлення причин пошкодження або джерела пошкодження. Запорукою виявлення та знешкодження таких ризиків є ефективна координація та співпраця на всіх рівнях Збройних Сил України.

Захист таємної інформації та зв'язку складається з:

розробки програмно-технічного забезпечення для запобігання порушень у кібернетичному просторі та впровадження ефективних алгоритмів роботи мереж;

сприяння відстеженню спроб злову захисту важливих інформаційних інфраструктур і надання інформації про результати такого відстеження іншим державам в разі необхідності;

впровадження технологій фізичного захисту приміщень, в яких базуються елементи інфраструктури від засобів акустичної розвідки, використання лазерних мікрофонів;

підготовки персоналу до швидкого реагування у разі порушення цілісності мереж (наприклад реагування на несанкціоноване врізання в мережу повздож кабелю);

запобігання потенційним розривам мережі шляхом створення бригад швидкого реагування, які мають чергувати у готовності до оперативного усунення причин порушення мережі;

наявності законів і кваліфікованого персоналу для розслідування спроб порушення захисту ключових інформаційних інфраструктур і притягнення до відповідальності причетних до цих спроб осіб, а також в належному порядку координування таких розслідувань з іншими державами та структурами.

Виходячи з того, що захист державної таємниці є одним із напрямків функціонування Збройних Сил України, перед ними постає завдання побудувати ефективну систему захисту в умовах лімітованого фінансування. Вирішити дане питання можливо шляхом використання комплексних систем захисту інформаційно-комунікаційних мереж, які довели свою ефективність, а також впровадженням високотехнологічних засобів передачі даних, що забезпечує захист інформації на всіх рівнях.

*Науковий керівник – А.В. Шашкін*