ОСНОВНІ МЕТОДИ КІБЕРЗАХИСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Ляшенко Г.Т., Бондаренко Т.В., Фомкін Д.В.
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ

Активне впровадження та функціонування інформаційних систем у діяльності Збройних Сил України зумовило виникнення нового виду бойових дій, що здійснюються у кіберпросторі. На сучасному етапі фіксується перша у світовій практиці повномасштабна кібервійна, до якої залучені військові підрозділи, державні установи, спеціальні служби та хакерські угруповання. Основними об'єктами кібератак виступають критично важливі елементи інфраструктури: інформаційно-телекомунікаційні системи підприємств енергетичного та комунального секторів, служби екстреного реагування, фінансова та логістична системи, а також інформаційні системи Сил оборони України.

Більшість інформації, що обробляється та зберігається в базах даних інформаційних систем, належить до категорії з обмеженим доступом. У зв'язку з цим забезпечення належного рівня кіберзахисту таких баз даних є одним із пріоритетних завдань структурних підрозділів, відповідальних за кібербезпеку.

Основні методи кіберзахисту:

- сегментація мережі та недопущення зберігання інформації у хмарі – для обмеження доступу та розподіл мереж на окремі сегменти для зниження ризиків;
- фізична безпека інформаційних систем – запобігання несанкціонованому фізичному доступу до обладнання та засобів зв'язку;
- використання засобів криптографічного захисту – шифрування переданої та збереженої інформації з використанням сертифікованих засобів;
- контроль доступу до систем – багаторівнева автентифікація, розмежування прав доступу та обмеження повноважень користувачів;
- захист радіоканалів та зв'язку – використання захищених протоколів, динамічна зміна частот і засобів радіоелектронної боротьби;
- системи моніторингу та реагування – постійний контроль активності, аудит інформаційних ресурсів та оперативне реагування на виявлені загрози;
- резервування та дублювання каналів зв'язку – забезпечення безперервності управління навіть за умов кіберінцидентів.

Висновки:

1. Ефективна кібероборона тактичного рівня неможлива без системного підходу – необхідно поєднувати фізичний, програмний, організаційний та криптографічний захист для гарантування стійкості систем управління до кібератак.
2. Критично важливим є впровадження багаторівневої системи контролю доступу – це дозволяє мінімізувати ризики несанкціонованого використання інформаційних ресурсів та обмежити можливість доступу ворога до тактичної інформації.