УДК 004.8:355

Оболонська Я. О.

ОРГАНІЗАЦІЯ ОСНОВ КІБЕРБЕЗПЕКИ У ВІЙСЬКОВИХ ПІДРОЗДІЛАХ

Анотація. *Досліджено організацію кібербезпеки у військових підрозділах, зокрема підготовку персоналу, технічний захист і реагування на кіберінциденти.*

Ключові слова: *кібербезпека, військові підрозділи, кіберзахист, інформаційна безпека, кіберінциденти, захист даних, кібергігієна, система безпеки.*

Abstract. *The organization of cybersecurity in military units was investigated, including personnel training, technical protection, and response to cyber incidents.*

Keywords: *cybersecurity, military units, cyber defense, information security, cyber incidents, data protection, cyber hygiene, security system.*

Вступ

В умовах збройної боротьби кіберпростір стає одним із ключових полів ведення війни. Кібератаки на інформаційні системи, центри управління, зв'язок і логістику військових структур становлять серйозну загрозу національній безпеці. Тому організація ефективної системи кібербезпеки у військових підрозділах є стратегічним завданням, яке передбачає створення єдиного комплексу технічних, організаційних та освітніх заходів. Вона спрямована не лише на запобігання кіберінцидентам, а й на своєчасне реагування, відновлення працездатності інформаційних систем та збереження бойової готовності підрозділів. Забезпечення належного рівня кіберзахисту вимагає підготовленого персоналу, сучасного технічного обладнання й чіткої координації дій усіх учасників кібероборони.

Результати дослідження

Організація основ кібербезпеки у військових підрозділах здійснюється через комплекс взаємопов'язаних заходів, спрямованих на створення безпечного інформаційного середовища, захист систем управління, комунікацій і даних від кіберзагроз. Основним завданням є формування у підрозділах єдиної політики кіберзахисту, яка визначає порядок доступу до інформаційних ресурсів, відповідальність посадових осіб, вимоги до технічного забезпечення та алгоритми дій у разі кіберінцидентів [1].

Першим елементом організації є нормативно-методична база, що встановлює стандарти, вимоги та процедури з кібербезпеки. У військових частинах діють внутрішні інструкції, положення та стандартизовані програми підготовки, який регламентує знання, що повинні мати військовослужбовці для безпечної роботи з цифровими пристроями і мережею. Ця база узгоджується з наказами Міністерства оборони, що визначають порядок впровадження технічних засобів захисту, моніторингу та реагування на кібератаки [2].

Другим елементом є освітньо-підготовча система. Кожен військовослужбовець проходить базовий курс із кібергігієни, який включає розпізнавання фішингових повідомлень, уникнення соціальної інженерії, безпечне користування гаджетами, паролями та службовими акаунтами [1]. Для командного складу організовуються спеціальні заняття з управління кіберризиками, виявлення вторгнень і реагування на інциденти. Підготовка здійснюється не лише теоретично, а й у формі практичних тренінгів, де відпрацьовуються сценарії кібератак і дій персоналу у кризових ситуаціях [2].

Третім складником є технічна організація кіберзахисту, що включає багаторівневу систему безпеки інформаційних ресурсів. У військових мережах застосовується шифрування даних, багатофакторна автентифікація, обмеження прав доступу, регулярне оновлення програмного забезпечення та аудит безпеки [1;2]. Системи виявлення вторгнень (IDS/IPS), фаєрволи та антивірусні засоби контролюють трафік і блокують підозрілу активність. Обов'язковим є створення резервних копій критичної інформації та збереження їх у захищених сегментах мережі.

Четвертий напрям є оперативне управління та реагування на кіберінциденти. У військових підрозділах створюються спеціальні групи або визначаються відповідальні особи за моніторинг стану інформаційної безпеки. У разі виявлення кібератаки запускається процедура локалізації, ізоляції заражених систем, аналізу причин інциденту та відновлення роботи мережі. Звіти про інциденти передаються у відповідні підрозділи кібероборони ЗСУ для централізованого аналізу та вдосконалення методів захисту [3].

П'ятий аспект контроль і вдосконалення системи кібербезпеки. Проводяться регулярні перевірки готовності персоналу, аудит безпеки мереж, тестування на проникнення і навчальні кіберманеври, метою яких є оцінка стійкості систем до атак [3]. Результати таких перевірок використовуються для оновлення політик безпеки, підвищення кваліфікації військовослужбовців та удосконалення технічних засобів.

Організація основ кібербезпеки у військових підрозділах базується на інтегрованому підході поєднанні нормативного регулювання, підготовки персоналу, технічного захисту, системного моніторингу та реагування на інциденти. Це забезпечує стійкість військових інформаційних систем, збереження бойової готовності та захист державних інтересів у кіберпросторі.

Висновки

Організація основ кібербезпеки у військових підрозділах є невід'ємною складовою обороноздатності держави. Ефективна система кіберзахисту базується на чітко визначених нормативних вимогах, високому рівні підготовки військовослужбовців, використанні сучасних технологічних рішень та постійному моніторингу безпекового стану мереж. Важливою умовою успішного функціонування є також налагоджена взаємодія між підрозділами кібероборони, технічними фахівцями та командуванням. Такий комплексний підхід дозволяє не лише своєчасно виявляти і нейтралізовувати загрози, але й формувати культуру безпечної поведінки у цифровому середовищі, що є запорукою надійного захисту військової інформаційної системи.

Список використаних джерел:

1. Sprotyv G7 - *інформаційний ресурс базових знань у військовій справі*. URL: https://sprotyvg7.com.ua/wp-content/uploads/2025/02/1_СТІ-000Г.97Л-ОСН-КІБЕР-КІП.pdf.
2. Основи кібербезпеки: як військовослужбовцям захиститися від ворожих кібератак. *Міністр оборони України.* URL: https://mod.gov.ua/news/osnovi-kiberbezpeki-yak-vijskovosluzhbovczyam-zahistitisya-vid-vorozhih-kiberatak.
3. Терновий, Шкуренко, Міненко. Перегляд Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України. *Сучасні інформаційні технології у сфері безпеки та оборони*. URL: https://sit.nuou.org.ua/article/view/278116/276052.

Оболонська Яна Олександрівна *– студентка групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, громадянка кафедри Військової підготовки, Вінницький національний технічний університет, Вінниця, e-mail: vn.oyana@gmail.com*

Obolonska Yana Oleksandrivna *- student of group 1BS-22b, faculty of information technologies and computer engineering, citizen of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vn.oyana@gmail.com*