будуть професійні навички операторів, знання специфіки території, на якій доводиться виконувати завдання, чітка взаємодія з цивільним населенням, вміння аналізувати непередбачувані ситуації та приймати рішення за умов обмеженого таймінгу. Саме українські військовослужбовці мають відповідний рівень підготовки та багаторічну практику для виконання окреслених задач.

Москалець Валентин Віталійович
викладач кафедри розвідки
доктор с.-г. наук, доцент, молодший сержант
Київський інститут Національної гвардії України

ЕШЕЛОНОВАНА АРХІТЕКТУРА РАДІОЕЛЕКТРОННОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ДОСВІД ПРОТИДІЇ КОМБІНОВАНИМ АЕРОДИНАМІЧНИМ ЗАГРОЗАМ

Досвід захисту української енергосистеми та промислових вузлів у 2022–2026 роках засвідчив, що класичні системи ППО не здатні самостійно гарантувати живучість об'єктів при масованих атаках. Виснаження дороговартісних зенітних ракет дешевими БпЛА-камікадзе робить радіоелектронну боротьбу (РЕБ) не просто допоміжним, а базовим елементом оборони територіального повітряного простору. Сьогодні ефективність захисту об'єктів критичної інфраструктури (ОКІ) базується на точному математичному розрахунку коефіцієнта придушення (K_j) у точці прийому сигналу цілю.

$$Kj = 10 \cdot log_{10} \frac{Pj}{Ps},$$

де Pj — потужність завади, Ps — потужність сигналу цілі.

Враховуючи використання противником завадостійких модулів із CRPA-антенами (наприклад, серії «Комета»), просте шумове загородження є неефективним. Науково обґрунтований захист вимагає створення енергетичного домінування завади на рівні 35–45 дБ, що реалізується через мережу синхронізованих випромінювачів, інтегрованих у єдине просторово-розподілене поле.

Побудова такої оборони має бути суворо ешелонованою, де кожен рубіж вирішує специфічні задачі деградації навігаційного рішення ворога. Дальній ешелон (30–50 км від об'єкта) фокусується на імітаційному впливі (спуфінгу) для внесення кумулятивної похибки в інерціальні системи крилатих ракет типу «Х-101» або «Калібр». Атаки на підстанції 750 кВ у Київській та Харківській областях показали, що навіть відхилення ракети на 30–50 м завдяки GPS-спуфінгу дозволяє зберегти автотрансформатори, переводячи основну енергію вибуху на допоміжні споруди (Defense Express, 2023). Подібні методи GPS-спуфінгу та ешелонованого РЕБ застосовувалися в Ірані проти американських дронів (2011 рік, випадок із RQ-170 Sentinel), а також у Сирії, де російські системи РЕБ впливали на навігацію БпЛА коаліції, що підтверджує актуальність для міжнародної практики. Аналіз цих ударів

демонструє практичну ефективність імітаційного впливу як першого ешелону оборони (табл.).

Таблиця. Функціональні рубежі ешелонованої архітектури РЕБ-захисту ОКІ

Ешелон	**Дистанція, км**	**Основні задачі**	**Технічні засоби**	**Очікуваний ефект**
Далекий	30–50	GPS-спуфінг	синхронізм-вані випромінюю-вачі	відхилення траєкторії КР («Х-101», «Калібр»)
Середній	5–15	бар’єрні завади	широко смугові генератори, антени 25–30 м	розрив каналів управління роїв БПЛА (433/900 МГц, 2.4/5.8 ГГц)
Термінальний	до 1	«електро магнітни й удар»	імпульсні передавачі високої потужності	фізичне виведення з ладу приймачів навіть у режимі «радіомовчання»

Ефективність захисту базується на створенні енергетичного домінування завади (35–45 дБ) через мережу синхронізованих випромінювачів. Архітектура має бути суворо ешелонованою (рис.).

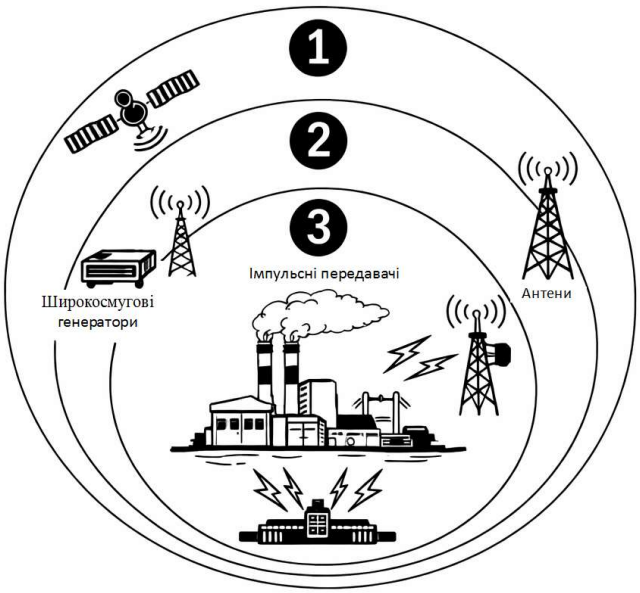

Рис. **Ешелонована архітектура радіоелектронного захисту об’єкта критичної інфраструктури:** 1. **Далекий ешелон (30–50 км)** – GPS-спуфінг для внесення похибки в навігаційні системи противника; застосовуються синхронізовані випромінювачі; 2. **Середній ешелон (5–15 км)** – бар’єрні завади для розриву каналів управління роїв БпЛА; використовуються широкосмугові генератори та антени

заввишки 25–30 м; 3. **Термінальний ешелон (до 1 км)** – «електромагнітний удар»; імпульсні передавачі високої потужності забезпечують фізичне виведення з ладу приймачів навіть у режимі «радіомовчання»

При переході загрози до середнього ешелону (5–15 км) система активує широкосмугові бар'єрні завади для розриву каналів управління роїв БпЛА (діапазони 433/900 МГц та 2.4/5.8 ГГц). На цьому етапі критичним є врахування «радіотіней» від промислових конструкцій – резервуарів нафтобаз чи машзалів ТЕС. Для ліквідації зон дифракції антенні пости необхідно розміщувати на щоглах висотою 25–30 м, забезпечуючи пряму радіовидимість цілі до самого горизонту.

Організація енергозабезпечення такої системи є окремим інженерним викликом, що вимагає виділених ліній живлення та автономних масивів безперебійного живлення. Наприклад, для комплексного прикриття великої ТЕС необхідно резервувати до 150 кВт потужності. Це дозволяє системі працювати в режимі «електромагнітного удару»: при виявленні цілі в термінальній зоні (менше 1 км) потужність випромінювання короткочасно зростає в рази, що призводить до фізичного виходу з ладу вхідних каскадів приймачів, навіть якщо дрон працює в режимі «радіомовчання» за інерціальною системою. При цьому фактор сезонності вносить корективи в розрахунки: низькі температури та висока вологість взимку покращують проходження хвиль, проте вимагають прецизійного термостатування електроніки для запобігання фазовим зсувам сигналу.

Особлива складність виникає при забезпеченні електромагнітної сумісності (ЕМС) з власними силами оборони. Неконтрольована робота потужного РЕБ поблизу великих міст призводить до «осліплення» радарів ППО та дезорганізації зв'язку мобільних груп. Вирішенням є цифрова синхронізація завадових імпульсів із робочими циклами дружніх РЛС (time-slotting). Окрім того, персонал об'єкта має бути готовим до протидії російським станціям технічної розвідки та РЕБ (типу «Житель» або «Поле-21»), які пеленгують вітчизняні випромінювачі. Це змушує переходити до тактики «радіозасідок», коли активна передача вмикається лише після верифікації цілі засобами акустичного чи оптичного моніторингу.

Отже, захист ОКІ сьогодні – це не статичний «купол», а динамічний, програмно-керований процес. Тільки поєднання глибокої ешелонованості, точних математичних розрахунків енергетичного бюджету та високої кваліфікації інженерного персоналу дозволяє створити зону, в якій сучасні засоби повітряного нападу втрачають свою головну перевагу – точність. Цей досвід, загартований у реальних бойових умовах, формує нові стандарти світової безпеки, де радіоелектронний простір стає основним рубежем оборони інфраструктури.