**ОСОБЛИВОСТІ ПОБУДОВИ БЕЗДРОТОВОЇ МЕРЕЖІ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

**ГАЧ В.С., студентка 2 курсу спеціальності «Кібербезпека»**

У сучасному суспільстві, що дедалі більше залежить від інформаційних технологій, надійність і безпека об’єктів критичної інфраструктури (ОКІ) є визначальними факторами національної безпеки. Бездротові мережі, як один із ключових елементів сучасних ІТ-систем, відіграють важливу роль у забезпеченні зв’язку та обміну даними між критично важливими підсистемами. У цій статті розглянуто особливості побудови бездротових мереж на об’єктах критичної інфраструктури з урахуванням вимог до стійкості, кіберзахисту та функціональної надійності.

Ключові слова: критична інфраструктура, бездротова мережа, кіберзахист, WLAN, безпека, проєктування мереж.

*Актуальність*. Зростання загроз кібератак, у тому числі на об’єкти критичної інфраструктури (ОКІ) - такі як енергетичні станції, транспортні вузли, медичні установи, підприємства оборонного значення - висуває високі вимоги до надійності інформаційних систем. Бездротові технології зв’язку забезпечують гнучкість, швидке розгортання та зниження витрат на інфраструктуру, проте вони є більш вразливими до атак, перешкод і несанкціонованого доступу. Саме тому особливої актуальності набуває питання правильного проєктування WLAN на ОКІ з акцентом на захист, стійкість до відмов і відповідність міжнародним стандартам кібербезпеки.

*Метою статті* є дослідження особливостей побудови бездротових мереж на об’єктах критичної інфраструктури з акцентом на пошук оптимальних рішень, що поєднують високу надійність зв’язку, стійкість до відмов, відповідність вимогам кібербезпеки та здатність до масштабування. Дослідження спрямоване на визначення технічних і архітектурних принципів проєктування WLAN, які забезпечують стабільну роботу інфраструктури в умовах підвищених ризиків, впливу зовнішніх факторів і можливих кібератак. Особлива увага приділяється вибору обладнання, топології мережі, засобам захисту та інтеграції з системами моніторингу й управління подіями безпеки.

*Об’єктом дослідження* є бездротова комп’ютерна мережа на об’єктах критичної інфраструктури.

*Предметом дослідження* є проєктні підходи, вибір обладнання, архітектура мережі та механізми кіберзахисту в умовах особливих вимог до стабільності та безпеки.

*Аналіз попередніх досліджень та даних.* Публікації останніх років вказують на активне впровадження бездротових рішень у сфері критичної інфраструктури. Згідно з матеріалами NIST та ENISA, організації дедалі частіше використовують Wi-Fi, LTE та 5G для збирання й передавання даних сенсорних систем, відеоспостереження, управління об’єктами SCADA. У звітах Cisco та Fortinet наголошується на потребі ізольованих сегментів WLAN, використанні WPA3-Enterprise, Network Access Control (NAC) та контролерів доступу. За даними досліджень Національного інституту кібербезпеки України, понад 70% інцидентів на ОКІ пов’язані з неправильними налаштуваннями мереж або слабкими паролями Wi-Fi. Це підкреслює необхідність застосування комплексного підходу до планування WLAN у таких умовах.

*Виклад основного матеріалу*. Бездротова мережа на об’єктах критичної інфраструктури (ОКІ) повинна відповідати суворим вимогам, що забезпечують її безперервну, захищену та відмовостійку роботу. Основні вимоги включають:

* Стійкість до відмов зв’язку: система має функціонувати у випадку втрати окремих вузлів або каналів зв’язку, що досягається через резервування обладнання та маршрутів передачі даних.
* Високий рівень шифрування та автентифікації: критично важливо запобігти несанкціонованому доступу до мережі або втраті конфіденційної інформації.
* Захист від перешкод і завад (електромагнітна сумісність): мережеві компоненти повинні мати захист від промислових завад (електродвигуни, радіохвилі, випромінення від обладнання).
* Підтримка безперервного моніторингу та журналювання: необхідна повна прозорість дій користувачів, пристроїв і мережевого трафіку для вчасного реагування на інциденти.

Архітектурні підходи до реалізації WLAN на ОКІ*:*

1. *Фізичне планування покриття*.

На етапі проєктування проводиться RF Site Survey - обстеження території для аналізу рівня сигналу, шумів і зон з поганим покриттям. Це дозволяє:

* виявити “мертві зони”;
* уникнути перекриття каналів (co-channel interference);
* забезпечити зону покриття 99,9% критичних точок (операторські, серверні, диспетчерські);
* врахувати ефект зони Френеля для передачі даних на відкритих ділянках.
1. *Вибір обладнання*.

Використовуються точки доступу промислового класу, що підтримують:

* Wi-Fi 6 / 6E (IEEE 802.11ax) – до 4.8 Гбіт/с;
* WPA3-Enterprise;
* PoE+ живлення (802.3at) для централізованого керування;
* роботу в умовах температур від –20 °C до +60 °C;
* захист від пилу та вологи (IP65–IP67).

Приклади обладнання:

* Cisco Catalyst IW6300 - призначений для промислових об’єктів;
* Ubiquiti UniFi U6 Enterprise - із підтримкою DFS-каналів та мульти-VLAN;
* Aruba AP-515 - підтримка Aruba Central, інтеграція з AI-based мережевим аналізом.
1. *Сегментація мережі*.

Рекомендується впровадження багаторівневої логічної сегментації:

* SCADA VLAN - ізольована, з мінімально можливим доступом до зовнішньої мережі;
* операторські VLAN - для ноутбуків, планшетів технічного персоналу;
* відеоспостереження VLAN - трафік RTSP/HTTP, потребує QoS;
* гостьова VLAN - з обмеженим доступом, фільтрацією за часом та трафіком;
* керуюча VLAN - для адміністрування пристроїв (NMS, SNMP, SSH).

Для безпеки між VLAN застосовуються міжмережеві екрани з ACL, а також контроль доступу на рівні 802.1X.

1. *Безпека WLAN.*

Для забезпечення високого рівня захисту впроваджуються:

* WPA3-Enterprise з авторизацією через RADIUS або LDAP-сервери;
* MAC-фільтрація з обмеженням підключення лише перевірених пристроїв;
* PKI-сертифікати (X.509) для автентифікації критичних систем;
* RBAC (Role-Based Access Control) - користувачам присвоюються ролі із визначеними правами доступу;
* WIPS-системи (наприклад, Aruba RFProtect, Cisco CleanAir) для виявлення:
1. фальшивих точок доступу (rogue AP),
2. атак «evil twin»,
3. деаутентифікаційних атак (deauth flood).
4. *Моніторинг і журналювання*.

З метою забезпечення нагляду й реагування впроваджуються:

* Zabbix, Nagios, PRTG - для моніторингу працездатності;
* Syslog-сервери - для централізованого збору логів з усіх пристроїв;
* інтеграція з SIEM-системами (QRadar, Splunk, Elastic Security) - для виявлення аномалій, збереження історії подій, кореляції даних;
* NetFlow/sFlow - аналіз мережевого трафіку, детектування сплесків активності, спроб сканування чи вторгнень.

*Висновки.* Побудова бездротових мереж на об’єктах критичної інфраструктури є складним та відповідальним завданням, яке потребує врахування численних технічних, організаційних та безпекових аспектів. Забезпечення безперервності роботи, стійкості до відмов та захисту від кіберзагроз можливе лише за умови комплексного підходу: ретельного планування покриття, використання сучасного промислового обладнання з високими стандартами безпеки, а також багаторівневої сегментації та постійного моніторингу мережі. Впровадження передових методів автентифікації, шифрування та контролю доступу дозволяє мінімізувати ризики несанкціонованого проникнення і забезпечити цілісність і конфіденційність даних. Отже, грамотне проєктування WLAN для ОКІ є ключовим фактором для підтримання національної безпеки та ефективного функціонування критичних систем у сучасних умовах кіберризиків.

**Використані джерела:**

1. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
2. ENISA. Guidelines on Securing Wireless Communications. <https://www.enisa.europa.eu/publications>
3. Aruba Networks. Securing Wireless for Mission-Critical Industrial Environments. <https://www.arubanetworks.com>
4. Cisco. Wireless Design Guide for Critical Infrastructure. <https://www.cisco.com>
5. Державний центр кіберзахисту України. Аналіз інцидентів на об’єктах критичної інфраструктури України, 2023.
6. IEEE Communications Magazine. Wi-Fi 6 for Industrial IoT, 2022.
7. Trend Micro Research. The Evolving Threat Landscape for Industrial Wireless, 2024. <https://www.trendmicro.com>