УДК 624.042

СУЧАСНІ ТЕХНОЛОГІЇ ФІЗИЧНОГО ЗАХИСТУ ОБ'ЄКТІВ (ОГОРОЖІ, БАР'ЄРИ, СИСТЕМИ КОНТРОЛЮ ДОСТУПУ)

Ірина РУДЕШКО, старший викладач кафедри державного нагляду у сфері техногенної та пожежної безпеки
Сергій ВОЛОЧАЄВ – студент факультету техногенної та пожежної безпеки
Національний університет цивільного захисту України

Актуальність. Фізичний захист об'єктів — це комплекс заходів, спрямованих на запобігання несанкціонованому доступу, вторгненням та іншим загрозам для людей, майна та інформації. Він включає як традиційні інженерні рішення (огорожі, бар'єри), так і сучасні технологічні системи (СКД, сенсори, інтегровані рішення) для підвищення рівня безпеки.

Сучасні підходи до фізичного захисту базуються на багаторівневому принципі побудови захисних зон, що включає зовнішні бар'єри, системи виявлення вторгнень і контролю доступу з ідентифікацією осіб.

Основна частина. *Фізичні огорожі і бар'єри*.

Периметрові огорожі. Периметрові огорожі — це перша лінія фізичного захисту, що створює фізичний бар'єр для потенційних правопорушників. Їхня ефективність підвищується за рахунок інтеграції з сенсорними та детекційними системами: датчики руху, кабельні чи оптоволоконні лінії тривоги, дозволяють не лише перешкоджати проникненню, а й виявляти спроби обходу або руйнування огорожі в реальному часі.

Електричні огорожі. Сучасні електричні огорожі надають немеханічний вплив на порушника, поєднуючи фізичний бар'єр з психологічним чинником стримування. Вони можуть бути обладнані тривожними системами, що відправляють сигнал у центр моніторингу при спробі порушення.

Болларди та бар'єри проти транспорту.

Для захисту від атак транспортних засобів використовуються болларди, шлагбауми, бар'єри з енергопоглинаючими властивостями, які здатні зупиняти автомобіль «в разі загрози». Такі рішення широко застосовуються в аеропортах, державних установах та комерційних об'єктах.

Системи контролю доступу (СКД / СКУД)

Системи контролю доступу (СКД) — це комплекс технічних та програмних засобів, що обмежують або дозволяють доступ до певних зон, приміщень чи ресурсів лише авторизованим особам.

Основним призначенням СКД є регулювання та моніторинг переміщення людей і транспорту, забезпечення безпеки об'єктів різного типу — від офісних приміщень до критичної інфраструктури.

Компоненти та технології

До складу сучасної СКД можуть входити:

- Ідентифікаційні пристрої: RFID / NFC зчитувачі, магнітні картки, QR-коди, біометричні сенсори (відбитки пальців, розпізнавання обличчя).
- Фізичні пристрої перекриття доступу: електромагнітні замки, турнікети, автоматичні ворота, шлагбауми.
- Програмне забезпечення для реєстрації подій, обліку часу, інтеграції зі службами безпеки.

Сучасні тенденції у СКД

Сучасні СКД активно розвиваються завдяки впровадженню:

- Біометричних технологій (підвищена безпека проти підробок).
- Безконтактних методів доступу через смартфони або смарт-карти.
- Хмарних сервісів для централізованого управління доступом і аналітики.
- Інтеграції з відеоспостереженням і аналітикою на основі ШІ для розпізнавання осіб і поведінкових патернів.

Інтегровані системи фізичної безпеки

Сучасні рішення фізичного захисту рідко працюють окремо — найчастіше це інтегровані системи, де СКД пов'язана з відеоспостереженням, датчиками вторгнення, сигналізаціями й центром моніторингу.

Завдяки такій інтеграції забезпечується:

- Єдина платформа управління безпекою;
- Автоматичне реагування на події (блокування доступу, тривожні сповіщення охороні);
- Аналітика та звітність для швидкого виявлення загроз.

Переваги та виклики сучасних технологій

Переваги

- Підвищений рівень безпеки завдяки багатофакторній ідентифікації.
- Автоматизація контролю та моніторингу без необхідності постійної присутності охоронців.
- Гнучкість у налаштуванні доступу відповідно до ролей та потреб.

Виклики

- Інтеграція різних систем від різних виробників потребує стандартів та сумісності (IP-технології, стандарт PSIA).
- Захист персональних даних та приватності у біометричних системах.
- Необхідність технічної підтримки та оновлення програмного забезпечення.

Висновки. Сучасні технології фізичного захисту об'єктів поєднують класичні інженерні рішення (огорожі, бар'єри) з передовими електронними та програмними системами контролю доступу та моніторингу. Це дозволяє створювати багаторівневі системи безпеки, що мінімізують ризики несанкціонованого доступу та оперативно реагують на загрози в реальному часі. Ефективне застосування цих технологій — один із ключових факторів для захисту критичних об'єктів, підприємств, громадських і приватних територій.

ЛІТЕРАТУРА

1. Про затвердження Загальних вимог до систем фізичного захисту ядерних установок та ядерних матеріалів : наказ Державного комітету ядерного регулювання України від 28.08.2008 № 156. – Офіц. вид. – Київ, 2008.

2. Про затвердження Методичних рекомендацій з організації фізичної безпеки об’єктів : наказ МВС України. – Офіц. вид. – Київ, 2023.
3. ДБН В.1.2-14:2018. Загальні принципи забезпечення надійності та конструктивної безпеки будівель і споруд. – Київ : Мінрегіон України, 2018. – 36 с.
4. ДСТУ EN 60839-11-1:2019. Системи тривожної сигналізації. Системи контролю доступу. Загальні вимоги. – Київ : ДП «УкрНДНЦ», 2019. – 45 с.
5. Гуменюк В. І., Кравченко О. М. Системи фізичного захисту об’єктів критичної інфраструктури // *Науковий вісник будівництва*. – 2021. – № 2. – С. 88–95.
6. Коваленко С. М. Інженерно-технічні засоби охорони периметра об’єктів // *Системи безпеки*. – 2020. – № 4. – С. 21–27.