Omelchuk, A. A. (2024). Providing access to bomb shelters using IoT. *Actual Issues of Modern Science. European Scientific e-Journal, 28*, 73-77. Ostrava: Tuculart Edition, European Institute for Innovation Development. (In Ukrainian)

DOI: 10.47451/inn2024-01-02

The paper is published in Crossref, ICI Copernicus, BASE, Zenodo, OpenAIRE, LORY, Academic Resource Index ResearchBib, J-Gate, ISI International Scientific Indexing, ADL, JournalsPedia, Scilit, EBSCO, Mendeley, and WebArchive databases.

Anton A. Omelchuk, Candidate of Technical Sciences (Ph.D.), Associate Professor, Department of Computer and Information Technologies and Systems. State Tax University. Irpin, Ukraine.
ORCID 0000-0001-6318-7464

Providing access to bomb shelters using IoT

Abstract: Civil protection is a function of the state aimed at protecting the population, territory, environment and property from emergencies by preventing such situations, eliminating their consequences and providing assistance to victims in peacetime and in a special period. The author deals with the issues of ensuring and technical organization of access to bomb shelters and shelters in the context of the invasion of the Russian Federation on the territory of Ukraine. The problems faced by the population of Ukraine during air alarms are analyzed. Concepts for improving bomb shelters through the introduction of automation tools and Internet of Things technologies are proposed. The author analyzes the problem of providing round-the-clock access to bomb shelters in conditions of a permanent missile threat. Three concepts for improving bomb shelters through the introduction of computerized control systems are proposed, two of which should provide the ability to quickly authenticate via the Internet.

Keywords: bomb shelter, controller, IoT, security, authorization.

Антон Анатолійович Омельчук, к.т.н., доцент, кафедра комп'ютерних та інформаційних технологій і систем. Державний податковий університет. Ірпінь, Україна.
ORCID 0000-0001-6318-7464

Забезпечення доступу до бомбосховищ за допомогою IoT

Анотація: Цивільний захист – функція держави, спрямована на захист населення, території, навколишнього природного середовища та майна від надзвичайних ситуацій шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період. У статті розглянуто питання забезпечення і технічної організації доступу до бомбосховищ і прихистків в умовах вторгнення Російської Федерації на територію України. Проаналізовано проблеми з якими стикається населення України під час повітряних тривог. Пропонуються концепції удосконалення бомбосховищ шляхом впровадження засобів автоматизації і технологій інтернету речей. У роботі проаналізована проблема забезпечення цілодобового доступу до бомбосховищ в умовах перманентної ракетної загрози. Запропоновано три концепції удосконалення бомбосховищ шляхом впровадження комп'ютеризованих систем управління, дві з яких мають забезпечувати можливість швидкої аутентифікації через мережу Інтернет.

Ключові слова: бомбосховище, контролер, IoT, безпека, авторизація.

Вступ

Цивільний захист – функція держави, спрямована на захист населення, території, навколишнього природного середовища та майна від надзвичайних ситуацій шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період.

З початком повномасштабного російського вторгнення, Україна, керуючись Кодексом цивільного захисту (*Кодекс…, 2017*), намагається забезпечити безпеку населення. Одним з напрямків діяльності є розвиток і розбудова мережі бомбосховищ, прихистків та пунктів надання допомоги. Хоча ці заходи загалом вже є ефективними, все ще залишаються певні організаційні проблеми які потребують термінового вирішення. Однією з таких проблем є питання цілодобової доступності бомбосховищ для людей.

Російська Федерація активно використовує терор мирного населення як засіб досягнення свої цілей (*Commission…, 2023*; *Bowen & Weed, 2023*). Тому держава-агресор регулярно завдає удари про цивільним об'єктам в Україні, використовуючи найрізноманітніші засоби ураження (балістичні і крилаті ракети, керовані та некеровані авіаційні бомби, реактивні системи залпового вогню, ствольну артилерію, ударні дрони). На всі ці типи загрози, або лише на їх потенційну можливість, державні служби України мають відповідно реагувати, оголошуючи повітряні тривоги (*Мапа…, н.д.*) під час вильотів російських ракетоносців і бомбардувальників, мета яких заздалегідь визначити важко. Крім того, Російська федерація активно використовує засоби радіо-електронної боротьби, зокрема імітуючи пуски ракет, щоб виявити розташування українських систем ППО або з метою послабити їх пильність. Враховуючи це, кількість повітряних тривог і їх загальна тривалість суттєво збільшується (*Таблиця 1*).

Результати дослідження

Цілком зрозуміло, що в умовах тривалого військового стану і постійних повітряних загроз пильність громадян знижується і відбувається звикання. Неодноразово виникали ситуації, коли відповідальні за бомбосховища особи, щоб запобігти спробам вандалізму, зачиняли її. Однак характер загроз, що виникають непередбачувано і розвиваються стрімко протягом кількох хвилин (*Рисунок 1*), обумовлює необхідність швидкого доступу до бомбосховища у різний час доби і злагоджених дій від усіх (*Прищепа, 2024*). Люди, виконуючи свої основні обов'язки на роботі, або під час відпочинку уночі, не можуть встигнути оперативно відреагувати на потенційну небезпеку. Таким чином, виникає задача забезпечення цілодобового доступу до бомбосховищ усіх бажаючих і при цьому обмеження доступу до бомбосховища, тоді, коли у цьому немає нагальних потреб.

Для вирішення розглянутої проблеми пропонується використовувати бюджетні контролери з підтримкою віддаленого керування електронними пристроями. У залежності від розташування бомбосховища і можливостей його користувачів, доцільно розглядати кілька основних варіантів побудови системи забезпечення доступу. Це може

бути технології API, Bluetooth, Wi-Fi, GSM, RFID, NFC або інша технологія, яка дозволяє передавати сигнали від користувача до дверей бомбосховища і навпаки (*Omelchuk et al., 2019*). У якості апаратного забезпечення для реалізації системи можна використовувати відомі рішення, такі як Arduino, Raspberry Pi, ESP32, NodeMCU або інші мікроконтролери та модулі, які підтримують обрану технологію зв'язку (*Rudakova et al., 2018*). Потрібно враховувати фактори, такі як дальність, швидкість, безпека, сумісність та вартість пристроїв і зв'язку. Також слід враховувати потенційну відсутність електроенергії і інтерент-з'єданання, тому система мусить мати можливість автономної роботи.

Першим варіантом є побудова автоматичної системи відмикання сховища під час оголошення повітряної тривоги. У такому випадку контролер, що керує замком, мусить мати постійний цілодобовий доступ до мережі інтернет і відслідковувати оголошення повітряної тривоги в області або місті.

Другим варіантом є встановлення системи, що немає доступу до мережі і використовує для доступу цифровий пароль або модуль RFID (*How…, 2022*). Така система є недорогою у виготовленні і обслуговуванні, велика кількість людей у разі небезпеки зможе відчинити сховище. Недоліком є те, що не всі особи, які потребують негайного захисту, знатимуть пароль чи матимуть відповідний модуль RFID і все одно потребуватимуть когось, хто має доступ. Хоч ця проблема набагато менша ніж у випадку з фізичним ключем. З іншого боку, така система не забезпечує високої захищеності сховища від вандалізму, адже пароль може знати велика кількість осіб.

Третім варіантом є комбінована автоматизована система, що може використовувати спеціального бота для популярних месенджерів, вебсторінку або додаток для Android. Зв'язати бота з замком дверей може бути досить складно, оскільки це вимагає наявності спеціального обладнання та програмного забезпечення. Потрібно перевірити, чи працює зв'язок належним чином, чи відповідає замок на команди бота, чи є якісь затримки, помилки, перешкоди або інші проблеми (*Rozov et al., 2019*). Необхідним є налаштувати параметри зв'язку, такі як ідентифікатори, паролі, ключі, токени, шифрування, аутентифікація, меню авторизації. Як і у першому варіанті система має бути під'єднана до мережі (*Ivanov et al., 2020*). Так само як і у другому варіанті, не всі особи зможуть потрапляти в сховище за бажанням, бо не матимуть змоги пройти авторизацію. Але наявність можливості у великої кількості людей пройти авторизацію і відчинити сховище дистанційно зводить ризики до мінімуму, при цьому на авторизовану особу покладається певна відповідальність, що має убезпечити бомбосховища від нецільового використання та вандалізму.

Дискусія

Війна постійно створює нові небезпеки і породжує нові виклики, що вимагають швидкої адаптації і гнучких підходів у вирішенні задач. Впровадження комп'ютеризованих систем різних типів має розвантажувати людей, дозволяючи їм виконувати більш важливі задачі. Такий підхід, за умови дотримання вимог до кібербезпеки, може бути прийнятний і для покращення функціональності бомбосховищ та забезпечення цілодобового доступу до них.

Висновки

Таким чином, у роботі проаналізована проблема забезпечення цілодобового доступу до бомбосховищ в умовах перманентної ракетної загрози. Запропоновано три концепції удосконалення бомбосховищ шляхом впровадження комп'ютеризованих систем управління, дві з яких мають забезпечувати можливість швидкої аутентифікації через мережу Інтернет.

Список джерел інформації:

Кодекс цивільного захисту України. (2017). *Офіційний вебпортал парламенту України*. [Code of Civil Protection of Ukraine. (2017). Official web portal of the Parliament of Ukraine. (In Ukrainian)]. https://zakon.rada.gov.ua/laws/show/5403-17#Text

Мапа тривог України. (н.д.). [Map of Alerts in Ukraine. (In Ukrainian)]. https://alerts.in.ua/

Прищепа, Я. (2024, 2 січня). П'ятеро загиблих, понад 120 поранених: які наслідки удару РФ по Києву та Харкову. *Суспільне. Новини.* [Prishchepa, Ya. (2024, January 2). Five dead, more than 120 wounded: What are the consequences of the Russian strike on Kiyv and Kharkiv? *Public. News.* (In Ukrainian)]. https://suspilne.media/652092-dvoe-zagiblih-desatki-poranenih-rosia-zavdala-raketnih-udariv-po-kievu-ta-harkovu/

Bowen, A., & Weed, M. (2023). *War crimes in Ukraine*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R47762

Commission of Inquiry finds further evidence of war crimes in Ukraine. (2023). *UN News*. https://news.un.org/en/story/2023/10/1142617

How to make a door lock security system with a Raspberry Pi board. (2022). *SriTu Hobby*. https://srituhobby.com/how-to-make-a-door-lock-security-system-with-a-raspberry-pi-board/

Ivanov, A., Kolosov, I., Danyk, V., Voronenko, S., Lebedenko, Y., & Rudakova, H. (2020). Design of multifunction simulator for engine room personnel training. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, *10*, 62-69. https://doi.org/10.35784/iapgos.1617

Omelchuk, A., Lebedenko, Y., & Polyvoda, O. (2019). Automated system for remote monitoring of the sprinkling machines status. *Applied Questions of Mathematical Modeling*, *3*, 77-93. https://doi.org/10.32782/2618-0340-2019-3-7

Rozov, Y. H., Rudakova, H. V., Omelchuk, A. A., Rusanov, S. A., Dmitriev, D. A., & Fedorchuk, D. D. (2019). Development of CAD/CAM/CAE Systems of Designing Spatial Frame for Technological and Machine-Tool Equipment. *IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 1-6. Ukraine: Polyana. https://doi.org/10.1109/CADSM.2019.8779277

Rudakova, H., Polyvoda, O., & Omelchuk, A. (2018). Using recurrent procedures in adaptive control system for identify the model parameters of the moving vessel on the cross slipway. *Data*, *3*(4), 60. https://doi.org/10.3390/data3040060

Appendix

Таблиця 1. Статистика повітряних тривог станом на 20.01.2024

Область / Громада	Загальна тривалість тривоги	Кількість тривог
Донецька область	148 д. 17 год. 37 хв.	3711
Запорізька область	129 д. 12 год. 6 хв.	3319
Волинська область	22 д. 10 год. 48 хв.	492
Львівська область	21 д. 7 год. 56 хв.	439
Полтавська область	67 д. 8 год. 34 хв.	1714
Харківська область	112 д. 6 год. 4 хв.	3252
Житомирська область	36 д. 17 год. 38 хв.	742
Хмельницька область	28 д. 19 год. 8 хв.	544
Херсонська область	64 д. 19 год. 8 хв.	1636
Сумська область	63 д. 22 год. 57 хв.	1511
Кіровоградська область	61 д. 8 год. 56 хв.	1494
Черкаська область	49 д. 16 год. 37 хв.	1107
Дніпропетровська область	89 д. 18 год. 26 хв.	2671
Київська область	43 д. 8 год. 46 хв.	850
Чернігівська область	51 д. 15 год. 37 хв.	952
Вінницька область	37 д. 7 год. 55 хв.	755
Одеська область	44 д. 3 год.	1033
м. Київ	41 д. 12 год. 8 хв.	845
Миколаївська область	80 д. 17 год. 6 хв.	1784
Закарпатська область	19 д. 9 год. 25 хв.	398
Тернопільська область	24 д. 14 год. 7 хв.	500
Чернівецька область	22 д. 7 год. 1 хв.	431
Рівненська область	24 д. 7 год. 58 хв.	509
Івано-Франківська область	21 д. 11 год. 14 хв.	433
Автономна Республіка Крим	406 д. 21 год. 13 хв.	9
Луганська область	659 д. 16 год. 7 хв.	2

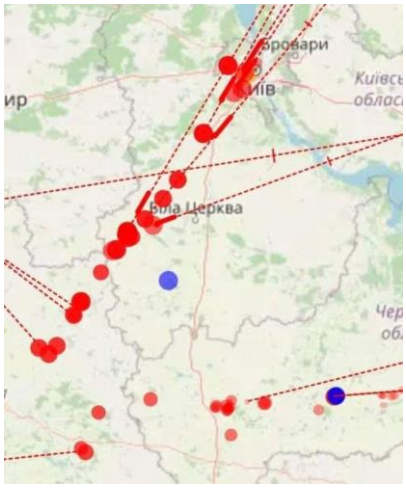

Рисунок 1. Мапа системи ЄППО під час ракетної атаки 12.09.2023