- з іншого боку, розвиток малогабаритних приймально-передавальних та інтелектуальних пристроїв (мікроконтролерів), здатних здійснювати обробку й бездротову передачу електричних сигналів, отриманих від сенсорів.

Науково-технічний прогрес останньої чверті XX століття створив передумови для широкого впровадження DCS у різноманітних сферах гуманітарної та виробничої діяльності. Одним із підтверджень таких досягнень стала реалізація на межі століть проєкту «Інтелектуальний пил» (Smart Dust), метою якого була розробка сенсорних вузлів (Sensor Node - Mote) розміром приблизно 1 мм³.

Мережевий рівень забезпечує передавання повідомлень між віддаленими вузлами мережі, тобто виконує функції маршрутизації, тоді як прикладний рівень визначає ієрархічну та сервісну роль вузлів, а також профілі виконуваних функцій. Стандарти IEEE 802.15.4 регламентують взаємодію трансіверів, тоді як специфікації ZigBee визначають принципи взаємодії мікроконтролерів [1].

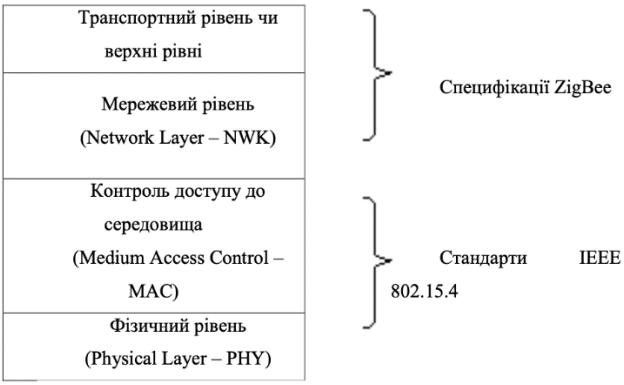

Рис. 1. Стек протоколів стандарту IEEE 802.15.4 і специфікації ZigBee

1. Охоронна сигналізація [Електронний ресурс]. – Режим доступу до ресурсу: http://www.florian-lviv.com/okhoronna-syhnalizatsiia.

Модель оцінювання кіберзахисту персональних даних у системах реєстрації заходів

УДК 004.056

Анна Васьковська[1], Євгенія Іванченко[2], Ігор Іванченко[3], Максим Марченко[4]

Державний університет інформаційно-комунікаційних технологій,
[1]a.vaskovska@duikt.edu.ua, [2]e.ivanchenko@duikt.edu.ua,
[3]i.ivanchenko@duikt.edu.ua, [4]mv.marchenko@duikt.edu.ua

У сучасному цифровому середовищі персональні дані є важливим інформаційним активом, а їх захист — одним із ключових завдань кібербезпеки. Бази реєстрації учасників спортивних подій обробляють значні обсяги конфіденційної інформації, зокрема ідентифікаційні дані, медичні довідки та платіжні реквізити, що робить їх привабливою ціллю для кіберзлочинців. Зі зростанням популярності онлайн-реєстраційних сервісів збільшується кількість кіберзагроз, серед яких фішингові атаки, компроментація облікових записів, ін'єкційні атаки, DDoS-атаки та експлуатація вразливостей веб-додатків. Успішна реалізація таких атак може призвести до витоку персональних даних, фінансових втрат і суттєвих репутаційних ризиків для організаторів спортивних подій.

Ефективний захист баз реєстрації потребує комплексного підходу, що включає використання багаторівневих механізмів безпеки відповідно до сучасних стандартів і рекомендацій, зокрема OWASP Top 10, NIST SP 800-53 та GDPR. Особливої актуальності це питання набуває в умовах підвищених кіберзагроз, характерних для України, де масові спортивні заходи проводяться в умовах постійного інформаційного протистояння. Враховуючи недостатній рівень впровадження сучасних механізмів захисту у більшості реєстраційних систем, актуальним завданням є розроблення моделі оцінювання рівня захищеності таких інформаційних ресурсів.

Метою цієї роботи є розроблення моделі оцінювання рівня захищеності персональних даних у базах реєстрації спортивних подій, що дозволяє виявляти вразливості та формувати рекомендації щодо підвищення кіберзахисту відповідно до сучасних стандартів інформаційної безпеки.

Сучасні реєстраційні системи для спортивних подій повинні відповідати високим вимогам інформаційної безпеки, оскільки обробляють значні обсяги конфіденційних даних. Одним із базових механізмів захисту є використання TLS (Transport Layer Security), який забезпечує шифрування каналу передачі даних між користувачем і сервером, а також гарантує цілісність інформації. Застосування HTTPS на основі актуальних версій TLS є стандартною вимогою для систем, що працюють із персональними та платіжними даними, оскільки дозволяють захистити їх від перехоплення та модифікації під час передачі.

Додатковими критичними елементами безпеки є багатофакторна автентифікація (MFA) та рольова модель доступу RBAC (Role-Based Access Control). MFA знижує ризик компрометації облікових записів шляхом використання кількох факторів автентифікації, тоді як RBAC обмежує доступ користувачів відповідно до їх ролей, мінімізуючи потенційні наслідки інцидентів безпеки. Сукупне застосування цих підходів забезпечує багаторівневий захист реєстраційних систем та підвищує стійкість до сучасних кіберзагроз.

Ще один критично важливий напрям забезпечення безпеки — моніторинг загроз і виявлення атак у режимі реального часу. Для цього застосовуються SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems) та журнали аудиту, які забезпечують фіксацію та аналіз усіх подій у системі.

Рис. 1. Алгоритм захисту персональних даних користувача в БР спортивних подіях

Попри наявність сучасних технологічних засобів захисту, організації, що проводять спортивні заходи, часто стикаються з обмеженістю ресурсів, відсутністю уніфікованих політик безпеки та впливом людського фактора. Це зумовлює необхідність впровадження моделей оцінювання рівня захищеності, які дозволяють об’єктивно визначати слабкі місця системи та формувати обґрунтовані заходи її вдосконалення.

1. Guide to Protecting Personally Identifiable Information (PII) // NIST. - URL:https://csrc.nist.gov/pubs/itlb/2010/04/guide-to-protecting-personally-identifiable-inform/final
2. Security and Privacy Controls for Information Systems and Organizations // NIST SP 800-53 Revision 5 Update 1. - URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final