Федоренко Д.П, магістрант,
Вакалюк Т.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

АНАЛІЗ ЗАГРОЗ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ РОЗУМНОГО ПАРКУВАННЯ

Сучасні системи паркування використовують передові технології для підвищення зручності, ефективності та безпеки. Зазвичай ці системи базуються на підключених до інтернету пристроях, таких як платіжні термінали, датчики, камери, мобільні додатки. Однак це робить їх вразливими до кібератак, які можуть порушити конфіденційність особистої інформації або порушити роботу системи[1].

Інтелектуальні системи паркування піддаються різноманітним загрозам і вразливим місцям, що можуть призвести до численних ризиків. Наслідки таких загроз можуть включати пошкодження інфраструктури паркування та порушення конфіденційної інформації користувачів.

Можливі кіберзагрози та їх протидії для систем розумного паркування включають [2]:

1. **Хакерські атаки та шкідливе програмне забезпечення:** Можуть викрасти дані, змінити платежі або порушити роботу системи.
Запобігання: Брандмауери, шифрування, регулярні оновлення, обмеження доступу та моніторинг.
2. **DoS-атаки:** Перевантажують систему трафіком, викликаючи збої або уповільнення, що призводить до затримок і порушення трафіку.
Запобігання: Захист від DoS-атак, виявлення та запобігання вторгненням, брандмауери.
3. **Внутрішні загрози:** Співробітники можуть свідомо чи несвідомо зловживати доступом, продавати дані або маніпулювати паркомісцями.
Запобігання: Перевірка персоналу, навчання кібербезпеці, мінімізація привілеїв доступу та аудит активності.
4. **Фішинг:** Зловмисники обманом отримують дані користувачів, такі як паролі чи платіжну інформацію, для несанкціонованого доступу.
Запобігання: Навчання користувачів розпізнавати фішингові атаки, багатофакторна автентифікація.
5. **Витоки даних:** Системи зберігають конфіденційні дані, які можуть бути викрадені для шахрайства чи крадіжки особистості.
Запобігання: Шифрування даних, контроль доступу, регулярні резервні копії та план реагування на інциденти.

Саме тому кіберпезпека відіграє ключову роль у забезпеченні захисту інформації та роботи систем розумного паркування, адже вона надає захист для фізичної інфраструктури паркінгу та персональної інформації користувачів. Крім того у разі компрометації системи паркування зловмисники можуть використовувати обладнання, наприклад, платіжні термінали чи камери відеоспостереження, створюючи потенційну загрозу громадськості.

Також важливим є постійна оцінка системи безпеки та її оновлення. Це повинно відбуватись як мінімум один раз на рік, однак, враховуючи постійне зростання та розвиток кібератак доцільно здійснювати їх частіше, наприклад, щоквартально[2].

Щоб зменшити ці ризики, системи паркування повинні бути спроектовані з урахуванням вимог безпеки та мати відповідні контрольні механізми для виявлення та усунення можливих загроз і вразливостей. Це може включати використання стандартів безпеки, таких як ISO/SAE 21434, ISO 27001, ISO 26262 та ISO 15408.Для подальшого розвитку важливо регулярно оцінювати ризики, пов’язані з системою, щоб своєчасно виявляти і усувати вразливості або потенційні загрози, які можуть призвести до атак[3].

Отже, кібербезпека є важливою складовою при розробці систем розумного паркування. Урахування безпеки на етапі проектування допомагає мінімізувати ризики, пов’язані з несанкціонованим доступом та іншими атаками. Попри все потрібно сприяти підвищенню рівня довіри з боку користувачів та ефективності розумних паркувальних систем у міських умовах. Тому безпека має бути інтегрована в усі етапи розробки, впровадження та експлуатації таких систем.

Список використаних джерел

1. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. (2018). SecSPS: A Secure and Privacy-Preserving Framework for Smart Parking Systems. *IEEE Transactions on Vehicular Technology*.
2. Cybersecurity for Smart Parking Systems URL: https://www.stackcache.io/tech/cybersecurity-for-smart-parking-systems/
3. Ibrahim, S., & SohrabiSafa, A. (2023). *Review on vulnerabilities and security challenges in autonomous vehicle systems*.