УДК 004

ВПЛИВ ТЕХНІЧНОГО РОЗВИТКУ НА СТРАТЕГІЇ ВИБОРУ ТА ОНОВЛЕННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ В ОФІСАХ ДОРОЖНЬО-БУДІВЕЛЬНИХ ОРГАНІЗАЦІЙ

Кононихін О.С., Прачик В.А.

Харківський національний автомобільно-дорожній університет, Харків

В сучасному світі дорожньо-будівельні організації стикаються зі зростанням вимог до технічної інфраструктури та мережевого обладнання. Це вимагає від них не лише ефективних стратегій вибору, але й постійного оновлення та удосконалення існуючих систем. Технічний розвиток і зростання конкуренції ставлять підприємства в умови, коли важливо не лише слідкувати за новими тенденціями, а й бути передовиками у впровадженні інновацій [1].

Однією з ключових аспектів технічного розвитку є швидкість передачі даних та висока пропускна здатність. В умовах дорожньо-будівельних організацій, де інформація щодо проектів, планів та технічних даних грає критичну роль, необхідно мати мережеве обладнання, що забезпечує швидкий та надійний обмін інформацією.

Вибір обладнання із високою пропускною здатністю дозволяє не лише оптимізувати робочі процеси, але й забезпечує ефективний моніторинг та управління проектами в режимі реального часу [1-2].

З поглибленням цифровізації та зростанням кількості підключених пристроїв, кібербезпека стає ключовим аспектом для будь-якої організації. Для дорожньо-будівельних компаній, які працюють з великою кількістю конфіденційної інформації, забезпечення кібербезпеки є критично важливим завданням [1-2].

Вибір та оновлення мережевого обладнання повинні враховувати сучасні технології захисту даних, мережеві фаєрволи та системи виявлення вторгнень. Це дозволяє уникнути потенційних загроз та забезпечує стабільну та надійну роботу мережі [1-2].

З впровадженням хмарних технологій стає можливим полегшення доступу до даних, спільна робота та зберігання інформації в онлайн-середовищі. Це особливо

важливо для дорожньо-будівельних проектів, що можуть охоплювати великі території та містити значну кількість графічних та технічних даних. Ключові елементи безпеки, які варто враховувати при виборі мережевого обладнання [1-3]:

- файрвол забезпечує захист мережі від несанкціонованого доступу. Повинен бути здатний фільтрувати трафік, контролювати доступ та виявляти загрози;

- антивірусне програмне забезпечення захищає від вірусів, шпигунського програмного забезпечення та інших загроз. Може бути реалізований на різних рівнях мережі;

- віртуальні приватні мережі захищають конфіденційність даних під час передачі через неприватні мережі;

- системи виявлення та запобігання вторгненням дозволяють виявляти та реагувати на спроби несанкціонованого доступу чи атаки;

- системи моніторингу мережі допомагають вчасно виявляти аномалії в мережевому трафіку, що може свідчити про можливі загрози;

- системи резервного копіювання та відновлення забезпечують безпеку даних шляхом регулярного резервного копіювання і можливості їх відновлення.

Перед вибором конкретного обладнання рекомендується провести аудит безпеки та визначити конкретні потреби організації. Також слід розглядати можливості масштабування обладнання в майбутньому, оскільки потреби в безпеці можуть зростати разом із збільшенням обсягу даних та розширенням мережі.

Вибір мережевого обладнання повинен враховувати можливість інтеграції з хмарними платформами, щоб забезпечити ефективний обмін даними та зручний доступ до інформації з будь-якого місця та пристрою.

Автоматизація та використання Інтернету речей можуть значно підвищити ефективність дорожньо-будівельних проектів. Встановлення сенсорів та IoT-пристроїв дозволяє збирати дані в режимі реального часу, відслідковувати стан обладнання та автоматизувати деякі процеси.

Важливо обирати мережеве обладнання, яке підтримує стандарти взаємодії з IoT-пристроями та може легко інтегруватися в системи автоматизації.

Вплив технічного розвитку на стратегії вибору та оновлення мережевого обладнання в дорожньо-будівельних організаціях важко переоцінити. Вибір сучасного та ефективного обладнання не лише поліпшує робочі процеси, але й забезпечує конкурентоспроможність компанії в умовах швидкої зміни технологічного середовища. Наведені вище аспекти врахування технічного розвитку допоможуть організаціям забезпечити стабільну та ефективну роботу своїх мереж і виявитися на висоті в умовах сучасного ринку.

Література:

1. Комп’ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] — Вінниця : ВНТУ, 2013. — 371 с.

2. Rajamohan P. An Overview of Virtual Router Redundancy Protocol Techniques and Implementation for Enterprise Networks / P. Rajamohan. – Selangor: SEGi University Kota Damansara, 2018. – 123 p.

3. Cisco AVVID Network Infrastructure Overview [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/web/offer/CAT4500/toolkit/comin_ov.pdf (Дата звернення 5.11.2023)