

доступу є розподіленим і захищеним від втручання, зменшуючи ризик несанкціонованого доступу, зміни або витоку даних.

Така інформаційна система захисту хмарних ресурсів дозволяє забезпечити децентралізований механізм контролю доступу до хмарних ресурсів на основі блокчейну та Distributed Ledger Technology, що забезпечує більшу безпеку хмарних обчислень та можливість прозорого та перевіреного журналювання та моніторингу цих систем.

УДК 004.056

ЗАХИСТ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА В РАДІОРЕЛЕЙНИХ ЛІНІЯХ ЗВ'ЯЗКУ

Роман Штонда¹, Юлія Черниш², Ірина Мальцева³

Військовий інститут телекомунікацій та інформатизації

імені Героїв Криму ¹roman.shtonda@viti.edu.ua,

²yuliia.chernysch@viti.edu.ua, ³iryna.maltseva@viti.edu.ua

Як показує наше сьогоднішнє, застосування радіорелейних ліній зв'язку (далі – РРЛЗ) не втратило своєї актуальності. Із початком повномасштабного вторгнення росії на територію України здійснено ряд кібератак, серед них було запущено шкідливе програмне забезпечення AcidRain, яке вплинуло на роботу станцій супутникового зв'язку Viasat. В результаті чого частина передачі даних лягла на РРЛЗ.

Метою даної роботи є доведення дій керівників установ/організацій щодо захисту інформації та кібербезпеки в РРЛЗ.

Радіорелейні засоби зв'язку та побудовані за допомогою них РРЛЗ не є чимось таким новим. Але кіберзагрози та кіберінциденти, що можуть в них виникати по тій чи іншій причині, є актуальним питанням котре потребує глобального вивчення та протидії. Керівники установ/організацій, що експлуатують та надають комунікаційні послуги за допомогою РРЛЗ повинні піклуватися про забезпечення надійного захисту інформації, що в них циркулює, а також здійснювати захист користувачів від кіберзагроз, що можуть проникнути в РРЛЗ із мережі Інтернет чи із-за необізнаного працівника.

Для вирішення даного питання, керівникам організацій/установ, необхідно проводити наступні дії: постійно проводити роботу з підлеглими працівниками з питань додержання кібергігієни; слідкувати за тим щоб працівники ніколи не залишали робочі пристрої (ноутбуки, планшети, накопичувачі тощо) без нагляду; розробляти та впроваджувати заходи додаткової верифікації при вході в мережу або систему; постійно застосовувати двофакторну автентифікацію під час підключення обладнання, яке призначене для роботи/налаштування РРЛЗ; застосовувати відповідні логіни та паролі та постійно проводити системне оновлення паролів доступу; застосовувати паролі із відповідною кількістю символів непов'язаних між собою; мати актуальне антивірусне програмне забезпечення постійно оновлювати його; на обладнанні встановлювати антишпигунське програмне забезпечення; застосовувати на всіх рівнях програмно-апаратні та програмні міжмережеві

екрани/брандмауери; мати в штаті центр захисту інформації та кібербезпеки; проводити систематичний моніторинг доступу до мережі Інтернет.

Підводячи висновок хотілось б зазначити, що для забезпечення розвитку радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання комунікаційних послуг, необхідно постійно приділяти увагу кібербезпеці під час побудови РРЛЗ. Додержання правил та вимог, які ми навели, дозволить будувати РРЛЗ з додержанням правил кібербезпеки та можливістю протидіяти витоку інформації. А також унеможливить проникнення кібершахраїв на робочі пристрої користувачів.

УДК 004.056.5

ВИКОРИСТАННЯ КВАНТОВОГО МАШИННОГО НАВЧАННЯ ПРИ ОБРОБЦІ БАГАТОКАНАЛЬНИХ АЕРОКОСМІЧНИХ ЗОБРАЖЕНЬ

Ірина Удовик¹, Володимир Гнатушенко²

Національний технічний університет «Дніпровська політехніка»

¹udovyk.i.m@nmu.one, ²vvgnat@ukr.net

Попередня обробка багатоканальних аерокосмічних даних та їх подальший аналіз є важливими задачами в багатьох прикладних областях, зокрема національна оборона та безпека покладаються на супутникові зображення як на важливе джерело інформації. Однак об'єм даних, який генерується за допомогою мульти- та гіперспектральних сенсорів на борту супутників дистанційного зондування Землі (ДЗЗ), а також радіолокаційних датчиків, продовжує зростати, перевищуючи 150 терабайтів на день. Для ефективного дешифрування значущої інформації з такого великого об'єму даних необхідні спеціальні інструменти та методи обробки великих даних. Алгоритми машинного навчання показали великий потенціал при аналізі даних ДЗЗ, проте результати цих технологій обмежені обсягом доступних навчальних даних та обчислювальної потужності. Для подальшого розвитку цих технологій необхідно забезпечити більш ефективну обробку та аналіз великих об'ємів геопросторових даних та використання нових методів машинного навчання, що дозволять отримувати більш точні та швидкі результати. Квантові алгоритми машинного навчання можуть допомогти вирішити зазначену проблему.

Метою дослідження є застосування квантових алгоритмів машинного навчання для аналізу великих об'ємів даних дистанційного зондування Землі. Актуальність даної теми полягає в тому, що ДЗЗ є важливим джерелом інформації для багатьох наукових, екологічних та господарських досліджень, а традиційні методи обробки цих даних є неефективними.

В роботі запропоновано використовувати квантові нейронні мережі з доступом до властивостей проєктованого квантового ядра (Projected Quantum Kernel – PQK) для класифікації зображень, розпізнавання об'єктів та піксельної сегментації.

Квантові комп'ютери з сотнями кубітів вже доступні науковій спільноті. Вони мають потужний потенціал для виконання складних квантових обчислень, що