УДК 519.71

**В. ХИЛЕНКО**
Національний університет біоресурсів і природокористування України, Київ, Україна; Словацький технічний університет, Братіслава, Словаччина, e-mail: *vkhilenko@ukr.net*.

**Б. АХМЕТОВ**
Казахський національний педагогічний університет імені Абая, Алмати, Казахстан.

**Р. БЕРДИБАЄВ**
Алматинський університет енергетики та телекомунікацій, Алмати, Казахстан.

**В. ЛАХНО**
Національний університет біоресурсів і природокористування України, Київ, Україна.

**Ю. ХАРЧЕНКО**
Національний університет біоресурсів і природокористування України, Київ, Україна.

**ВЕН-ЛІАНГ ХВАНГ**
Інститут інформаційних наук, Academia Sinica, Тайбей.

**В. ХИЛЕНКО мол.**
Словацький технічний університет, Братислава, Словаччина.

# ПІДВИЩЕННЯ ШВИДКОДІЇ БАНКІВСЬКИХ СИСТЕМ КІБЕРБЕЗПЕКИ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ ТА АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ КІБЕРАТАК. Ч. 1

**Анотація.** Розглянуто підвищення швидкодії та якості роботи систем кіберзахисту банківських установ в умовах постквантумної ери. Запропоновано математичний апарат для систем прогнозування кібератак та алгоритм визначення моменту включення режиму підвищеної захищеності. Враховано можливість організації кібератак за допомогою нейромереж та алгоритмів штучного інтелекту. Наведено приклад формування та аналізу кластера підозрілих операцій із використанням мови Julia.

**Ключові слова:** кіберзахист банківських установ, загрози постквантумної ери, система прогнозування кібератак, запобігання кібератакам, кластеризація.

Природний розвиток та вдосконалення апаратних засобів, насамперед розвиток квантових комп'ютерів та програмного забезпечення, а також поява нових технологій — технологій штучного інтелекту (ШІ), підвищують загрози кібератак на банківські установи, а статистика свідчить про збільшення втрат банківських установ, спричинених кібератаками. Тому зростає важливість удосконалення та підвищення якості систем кіберзахисту банків та фінансових установ. Це зумовлює потребу раннього виявлення можливих напрямків атак та обходу контрольних (захисних) алгоритмів системи кібербезпеки. Упровадження таких аналітичних підсистем (підблоків) «раннього запобігання», що прогнозують у реальному режимі часу можливу підготовку кібератак до систем кібербезпеки банківських установ, потрібне для зменшення часу реагування на початок кібератак, раннього припинення розвитку негативних процесів (операцій) і мінімізації заподіяної шкоди.

Вважатимемо, що загальна база даних (БД) та інформаційні потоки банківської установи відповідають принаймні двом параметрам, які дають змогу стверджувати про їхню належність Big Data [1, 2]: показнику обсягу даних та показнику швидкості їхньої модифікації. З огляду на це однією з розглядуваних проблем ефективності систем кібербезпеки є оперативне виявлення даних, що вказують на спроби дестабілізації системи кібербезпеки та можливої підготовки до кібератаки. Аналіз таких даних з урахуванням прогнозів стійкого функціонування банківської установи в нормальному режимі потрібен для оперативного