мами на основі використання лексичної бази даних *WordNet* (акад. НАН України П.І. Андон).

Фахівці Інституту інформаційних технологій та систем НАН України створили комп'ютерно-телекомунікаційний комплекс з оброблення даних сенсорів для автономної навігації БпЛА та тренажер для операторів. Комплекс сертифіковано Міністерством оборони України (О.Є. Волков, Д.О. Волошенюк, М.М. Комар).

КІБЕРБЕЗПЕКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Науковці Інституту кібернетики імені В.М. Глушкова НАН України розробили швидкі алгоритми виконання операцій над *s*-слівною арифметикою для розв'язання задач двоключової криптографії (шифрування, дешифрування, ЕЦП та його верифікація) і задач трансобчислювальної складності в галузі кібербезпеки. Аналогів у світі немає (акад. НАН України В.К. Задірака, А.М. Терещенко, І.В. Швідченко).

Розроблено строге математичне формулювання способу визначення можливої дезінформації у процесі обміну повідомленнями та статистичні критерії для перевірки користувачем наявності дезінформації в повідомленнях. Результати призначено для ефективнішого вибору стратегій учасників обміну інформацією з урахуванням її цінності та можливої дезінформації (чл.-кор. НАН України М.М. Савчук).

Розроблено технологію аналізу поведінки великих програм для виявлення вразливостей у програмному та апаратному забезпеченні об'єктів критичної інфраструктури. Реалізовано метод ефективного відокремлювання частини програмного коду, який зберігає здійсненність заданого сценарію поведінки. Метод призначено для аналізу програмного забезпечення об'єктів критичної інфраструктури, що містить різноманітний стек викликів або складну рекурсію. Технологію розгорнуто на паралельній версії платформи на основі сімейства суперкомп'ютерів СКІТ (О.О. Летичевський).

Фахівці Інституту проблем реєстрації інформації НАН України проаналізували підходи та методи підвищення функціональної стійкості ІС критичних інфраструктур з урахуванням можливості реалізації кібератак. Для зниження ризиків виникнення і поширення надзвичайних ситуацій у критичних інфраструктурах запро-

поновано створювати їх інформаційну інфраструктуру шляхом інтеграції ІС критичної інфраструктури в рамках побудови єдиного інформаційного простору. Напрацьовано методику і практичні рекомендації щодо його побудови в умовах інформаційної неповноти та жорстких вимог щодо зменшення впливу людського фактору під час вирішення завдань багаторівневого оброблення інформації. Запропоновано способи відновлення частково втрачених даних, що стосуються об'єктів моніторингу (О.Г. Додонов, О.М. Буточнов, О.С. Горбачик, В.О. Додонов, М.Г. Кузнєцова, Є.О. Цибульська, В.В. Юзефович).

Створено технології розпізнавання та аналізу загроз, що підвищують стійкість інформаційно-комунікаційних систем різного призначення, зокрема завдяки використанню алгоритмів штучного інтелекту (О.Г. Додонов, В.О. Додонов, В.Г. Путятін, С.А. Купенко).

В Інституті інформаційних технологій та систем НАН України розроблено метод, що базується на сучасних досягненнях криптографії з відкритими ключами для автентифікації — типового завдання інформаційно-комунікаційних технологій, що дало змогу формувати цифрові підписи, які неможливо підробити, блокчейн технології надійного зберігання інформації, розподілені децентралізовані мережі з елементами штучного інтелекту (акад. НАН України А.В. Анісімов).

Уперше в Україні розроблено модель представлення семантики речень для прикладних завдань комп'ютерної лінгвістики та методи кодування текстів з метою отримання компактного векторного представлення, що гарантує виконання вимог векторної семантики для визначення тематики та емоційної направленості текстів (акад. НАН України А.В. Анісімов, О.О. Марченко).

Науковці Інституту телекомунікацій і глобального інформаційного простору НАН України розробили псевдоквадратичні публічні ключі криптографії від багатьох змінних, що визначаються поліноміальними відображеннями n-вимірного афінного простору над скінченим арифметичним кільцем лишків за модулем m або скінченим полем. Такий постквантово стійкий алгоритм доповнено протоколом некомутативної криптографії, що дає змогу переводити публічний ключ у криптосистему типу Ель-Гамаля (В.О. Устименко).

Створено нові криптографічні протоколи з блокчейн-ядром, що вирізняються підвищеною стійкістю до криптоаналізу та швидкодією, децентралізовану систему раннього виявлення вторгнень на основі безшаблонного виявлення аномалій і збереження репутації в блокчейні, отримано нові оцінки стійкості класичних протоколів криптовалют (чл.-кор. НАН України А.М. Кудін).

Створено сучасну навчальну платформу «Лабораторія Автоматизованої системи керування», метою якої є підвищення розуміння професіоналів сучасних методів захисту загалом і захисту промислових систем управління (*ICS*) та систем диспетчерського контролю та збору даних (*SCADA*), що досягається шляхом глибокого практичного навчання та підвищення кваліфікації в лабораторії *ICS* (чл.-кор. НАН України О.М. Новіков).

Розроблено методи оцінювання рівня кіберзахисту та підвищення стану кіберзахисту об'єктів критичної інфраструктури держави, які допомагають автоматизувати процес оцінювання стану кіберзахисту на об'єктах огляду. Запропоновано структурну модель оцінювання стану кіберзахисту об'єктів критичної інфраструктури, що уможливлює реалізацію процесу оцінювання рівня їхнього кіберзахисту у слабоформалізованому нечіткому довкіллі та автоматизацію процесу оцінювання підвищення зазначеного стану (чл.-кор. НАН України О.Г. Корченко, Державний університет інформаційно-комунікаційних технологій).

ЦИФРОВА МЕДИЦИНА

Науковці Інституту кібернетики імені В.М. Глушкова НАН України створили кластер високої доступності для Хмарної платформи пацієнтцентричної телереабілітації онкологічних хворих для мінімізування простою системи, що знижує ризики відмов у роботі через надмірне навантаження або апаратні збої. Таке рішення забезпечує можливість оброблення даних про пацієнтів через інтелектуальні системи підтримки ухвалення рішень і забезпечує цілодобовий доступ до реабілітаційних сервісів (акад. НАН України О.В. Палагін, К.С. Малахов).

Спільно з Державною науковою установою «Науково-практичний центр профілактичної та клінічної медицини» Державного управління справами розроблено моделі визначення ризику смерті