На зовнішньому рівні безпеки (відбір/контроль інформації) виникають загрози: відмова та несправності технічних засобів, пошкодження у зв'язку з погодними умовами, установка закладних пристроїв, порушення режиму конфіденційності, режиму охорони і системи захисту, виведення давачів з робочого стану. Зовнішня безпека системи «Розумний будинок» передбачає використання систем: біометрії, відеоспостереження, радіочастотної ідентифікації, контролю доступу т. і.

На внутрішньому рівні (аналіз, автоматизація обробки інформації з обмеженим доступом, прийняття управлінського рішення) виникають загрози: порушення цілісності та достовірності інформації, витік інформації при зберіганні, навмисне викрадання даних, несанкціонований доступ до інформації. Технологіями захисту на внутрішньому рівні безпеки є: підвищення рівня системи безпеки, постійне оновлення системи безпеки, моніторинг доступних користувачів, використання ліцензійного програмного забезпечення, постійне оновлення програмного забезпечення, використання алгоритмів шифрування AES, "Калина".

Висновок. Розглянуто застосування КФС у проектуванні системи "Розумний будинок" на рівні структури контроль – обробка – управління, а також модель інформаційної безпеки відповідно до концепції "загроза – захист."

Х. Руда
Науковий керівник – д.т.н., проф. Г. В. Микитин

ВИКОРИСТАННЯ ПРЕДИКТИВНИХ МОДЕЛЕЙ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТАМИ

Сучасні банківські системи дозволяють клієнтам оперувати коштами, використовуючи численні способи, зокрема платежі через Інтернет, для виконання яких необхідні тільки реквізити, які фізично розташовані на пластиковій картці. Зловмисник, використовуючи засоби соціальної інженерії або технічні засоби, може дізнатись реквізити і спробувати використати їх для власного збагачення. Спеціалізовані структури банку аналізують деталі транзакції і авторизують або не авторизують її. Під час проведення аналізу проблемою є відносно невелика кількість підтверджених шахрайських запитів в порівнянні із загальною кількістю операцій.

Актуальною є задача балансування наборів даних, що використовуються для класифікування транзакцій шахрайськими або не шахрайськими.

У роботі розглядається ефективність використання двох методів штучного балансування даних для використання їх у задачах класифікації. Крім того, було протестовано 4 методи класифікації, що дало змогу вибрати найкращий з них для даного датасету. Окремо виділено проектування класифікаційної нейронної мережі. Параметри всіх класифікаторів, а також штучної нейронної мережі вибирались методом пошуку сіткою, що дозволило однозначно виявити оптимальні для даного набору даних. Розроблене рішення пропонується використовувати як фреймворк для застосування на реальних наборах даних.

Балансування датасету відбувалось двома методами: випадковим вибором даних з більшого класу у кількості, що дорівнює кількості зразків, що належать меншому класу та SMOTE-стратегія, що синтетично збільшує кількість зразків міноритарного класу.

Первинний датасет містив 31 категорію, в одній з яких були записані вихідні дані (шахрайська чи не шахрайська), а інші включали в себе різного роду деталі транзакції, що становлять множину описів об'єктів. Кількість об'єктів у початковому наборі даних – 284806, з яких до міноритарного класу належить 492, а до мажоритарного – 284314. По 20% об'єктів кожного класу були відокремлені для того, щоб використовуватись в тестуванні. Значення були попередньо відрегульовані відповідно до політики оперування персональними даними, тому додаткове масштабування не виконувалось. Обробка даних, моделювання, тестування і візуалізація результатів виконувались засобами мови програмування Python і додатковими бібліотеками.

Після балансування отримали два набори даних – undersampled dataset (788 об'єктів) та SMOTE (454902 об'єкти), кожен з яких містить рівну кількість об'єктів кожного класу.

Вибір класифікатора проводився з-поміж 4 схем предиктивних моделей: логістична регресія, k-НС, дерево рішень та метод опорних векторів. Моделі тестувались на undersample датасеті, а їхня точність оцінювалась методом ROC-кривих. Найточніші результати показав класифікатор на базі методу логістичної регресії.

Проектована нейронна мережа за структурою є перцептроном з одним прихованим шаром. Такі мережі є традиційними для вирішення задач простої класифікації. Навчання відбувається методом зворотного поширення помилки.

Проведено тестування наборів даних за допомогою класифікатора та нейронної мережі на даних, що не застосовувались для тренування. Ефективність роботи предиктивних моделей оцінювалась кількістю помилок другого роду. Результати тестування наведено на рисунку 1.

	Класифікатор	Нейронна мережа
Undersample	12	8
SMOTE	18	16

Рис. 1. Результати оцінки помилок другого роду

На рисунку представлені абсолютні значення кількості пропущених шахрайських запитів, тоді як загальна кількість шахрайських запитів, що мали бути виявлені, становить 98.

Висновок. Розроблені моделі класифікації на основі штучно збалансованих наборів даних показали ефективність використання обидвох методів для тренування класифікаторів або класифікаційних нейронних мереж.

О. Тимошенко
Науковий керівник – д.т.н., проф. Л. В. Мороз

МЕТОД ШВИДКОГО ОБЧИСЛЕННЯ ІНВЕРСНОГО $\sqrt{x}$ ДЛЯ ЗНАЧЕНЬ ТИПУ FLOAT

Обчислення нормалізованих векторів для комп'ютерної графіки є досить складною задачею навіть для потужних сучасних комп'ютерів. Оскільки програма з 3D графікою використовує їх для визначення освітлення і відображення, мільйони цих обчислень повинні виконуватися за секунду. Нормалізація вектора це домноження кожної його координати на величину $1/\sqrt{x^2 + y^2 + z^2}$.

На відміну від додавання та піднесення до степеня розрахунок квадратного кореня та ділення – складні для процесора операції. Саме тому **актуальною є задача** розробки алгоритмів швидкого обчислення оберненого квадратного кореня для чисел з рухомою комою.

На початку 1990-х років співробітники компанії Silicon Graphics винайшли алгоритм InvSqrt1, на основі якого в 2018 році було розроблено алгоритм InvSqrt2, який описано в статті Improving the accuracy of