розуміння того, що об'єкт є одним і тим же, якщо дивитися на нього з нової точки зору.

Капсульні мережі направлені на усунення недоліків сучасних систем машинного навчання, які обмежують їх ефективність. В цьому підході використовуються невеликі групи нейронів, які називаються капсулами. В свою чергу, капсули складають шари для ідентифікації об'єктів на відео або зображеннях. Коли декілька капсул в одному шарі приймають однакове рішення, вони активують наступну капсулу, що знаходиться на рівень вище. Цей процес продовжується доки мережа не зможе зробити висновок про те, що вона бачить. Кожна із капсул КМ створена таким чином, що здатна виявляти у зображенні конкретну ознаку і розпізнавати її під різним кутом.

Капсульні мережі потребують менший об'єм даних для навчання та розпізнавання об'єктів у нових ситуаціях. Вони не поступаються звичайним ШНМ у розпізнаванні рукописних символів. КМ пройшли тест на розпізнавання об'єктів, що були зображені з різних ракурсів, та зробили в два рази менше помилок ніж інші мережі.

Проте на даному етапі розвитку КМ поступаються традиційним ШНМ у швидкості обробки даних, що потребує подальшого вивчення та вдосконалення технології капсульних мереж.

Захист WEB-порталів спеціалізованих інформаційних систем Національної поліції України

Мазенко Н.А.
курсант 4-го курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Мирошниченко В.О.
науковий керівник, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

На теперішній час неабиякий вплив здійснюють не лише соціальні, політичні та економічні течії, а насамперед інформаційний потік інформації. Інформаційний вплив здатен уражувати будь-який пласт не лише суспільства, а й держави в загалом. Впровадження нових

інформаційних систем призвело не лише до підвищення рівня інформаційних технологій, а й до створення нових проблем інформаційного середовища. Важливим напрямком підвищення ефективності функціонування спеціалізованих інформаційних систем Національної поліції (НП) є інтегрування з глобальною мережею Internet. У багатьох випадках завдяки, власне ступеню інтегрування, вирішуються дві основні задачі. По-перше, об'єднуються територіально розподілені підсистеми інформаційних систем (ІС). По-друге, користувачам Internet забезпечується доступ до відкритої інформації ІС. Досить часто при розв'язанні обох задач використовується Web-сайт (Web-портал), який, у свою чергу є провідним серед інших інформаційних систем у мережі Інтернет [1, с.146].

Якщо звернутися до практичної діяльності, то треба зазначити, що функціонування окремого WEB-порталу відіграє свій вплив на функціонуванні усієї інформаційної системи. Основною ланкою WEB-порталу є Web-сервер, який забезпечує доступ користувачів із мережі Internet до Web-сторінок порталу.

Однак, в практиці зустрічаються випадки, коли безпека інформації зазнає впливу негативних уразників. Такими випадками порушення безпеки інформації є:

- блокування інформації (дії, наслідком яких є припинення доступу до інформації);
- несанкціонований доступ (доступ до інформації, що здійснюється з порушенням установлених в ІС правил розмежування доступу);
- витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації (дія, внаслідок якої інформація в ІС припиняє своє існування для фізичних або юридичних осіб, які мають право власності на неї в повному або обмеженому обсязі);
- модифікування інформації (умисні дії, які призводять до деформації інформації, яка має оброблятися або зберігатися в ІС);
- порушення роботи ІС (дії або обставини, які призводять до спотворення процесу оброблення інформації)

Саме тому керуючий особовий склад підрозділів Національної поліції України під час процесу створення будь-яких WEB-порталів та при цьому визначає операторів, вузли яких будуть використовуватись для налаштування під'єднання до мережі Internet, керуючись при цьому

не лише законами України та іншими нормативно-правовими актами, а й базою даних, що встановлює вимоги забезпечення з технічного захисту інформації (ТЗІ) та передовим практичним досвідом стосовно розроблення новітніх інформаційних методів і процесів захисту інформації [2, с.372]. Будь-який із WEB-порталів може бути розміщений на власному сервері, або ж на сервері, який визнається власністю оператора. На певного власника серверу покладається обов'язок гарантувати власнику інформації певний рівень встановленого захисту, досягається це тим, що функціонування WEB-порталу забезпечується ІС, в якій створюється комплексна система захисту інформації (КСЗІ), яка є сукупністю організаційно-правових та інженерно-технічних заходів, а також програмно-апаратних засобів, які безпосередньо і забезпечують захист інформації [3, с.293].

Нормальне функціонування Web-порталу, під'єднаного до мережі Internet, практично неможливе, якщо не надавати належну увагу кожній проблемі забезпечення його інформаційної безпеки. Найефективніше ця проблема може бути вирішена шляхом застосування комплексного підходу до захисту інформаційних активів порталу від можливих інформаційних нападів. Для цього до складу комплексу засобів захисту порталу повинні входити підсистеми антивірусного захисту, виявлення втручань, контролю цілісності, криптографічного захисту, розмежування доступу, а також підсистема управління. При цьому кожна з підсистем повинна бути оснащена елементами власної безпеки.

1. Кулешник Я. Ф. Основні завдання захисту інформації в операційних системах / Я. Ф. Кулешник, Т. В. Рудий, І. В. Бичинюк, Д. М. Неспляк // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності органів Національної поліції,– Львів: 2016. – С. 145–148.

2. Захаров В. П. Проблеми інформаційного забезпечення правоохоронних структур: навчальний посібник / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2011. – 372 с

3. Андреєв В. І. Основи інформаційної безпеки: підручник для студентів ВНЗ які навчаються за напрямом «Інформаційна безпека» / В. І. Андреєв, В. О Хорошко, В. С. Чередниченко, М. Є. Ше- лест; за ред. В. О. Хорошко. – К.: ДУІКТ, 2015. – Вид. 2-ге, доп. і переробл. – 293 с.