РОЗДІЛ ІІ.
ДОСВІД ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ЗАПОБІГАННЯ ПРАВОПОРУШЕННЯМ

2.1. Використання технологій штучного інтелекту в сфері безеки дорожнього руху.

За даними Всесвітньої організації охорони здоров'я, дорожньо-транспортний травматизм наразі є однією з найбільших проблем охорони здоров'я, і, за прогнозами, у 2030 році ДТП може стати однією з основних п'яти причин смертності людей у світі[38]. В Україні рівень смертності та травматизму внаслідок ДТП є одним із найвищих в Європі, а рівень організації безпеки дорожнього руху залишається вкрай низьким. Починаючи з 2015 року в Україні кількість аварій невпинно зростає. До прикладу у 2015 та 2016 роках було зафіксовано майже 140 тисяч ДТП, а вже у 2017 – вже 162 тисячі. У 2020 році на українських дорогах трапилось понад 168 тисяч ДТП. За цей рік загалом загинула 3541 людина, зокрема 168 дітей, 1198 пішоходів та 235 велосипедистів і 31974 людини дістали травм[39].

Протяжність автомобільних державних доріг в Україні становить 169,5 тис. км. і держава не може забезпечити присутність патрульних поліцейських або іншої уповноваженої особи на кожному кілометрі дороги для контролю за безпекою дорожнього руху. Так само неможливо забезпечити індивідуальний контроль за кожним учасником дорожнього руху. Тому системи

[38]Application of Artificial Intelligence in Traffic Control System of Non-Autonomous Vehicles at Signalized Road Intersection. August, 2020. Procedia CIRP 91. URL: https://www.researchgate.net/publication/343725566_Application_of_Artificial_Intelligence_in_Traffic_Control_System_of_Non-Autonomous_Vehicles_at_Signalized_Road_Intersection.
DOI: 10.1016/j.procir.2020.02.167

[39]У 2020 році кількість ДТП зросла майже на 8 тисяч. URL: https://www.pravda.com.ua/news/2021/01/13/7279729/

ШІ зможуть значно підвищити безпеку дорожнього руху на дорогах України про що засвідчує як вітчизняний досвід, так і досвід багатьох іноземних держав.

2.1.1. Міжнародний досвід

В **США** компанія Startup Waycare Technologies випустила інтелектуальну технологію Waycare, яка випробовується для попередження аварій у США. Їх

система поєднує дані в реальному часі з камер дорожнього руху, датчиків та додатків для повідомлення про дорожній рух з історичними даними для аналізу тенденцій та прогнозування часу та місця майбутніх аварій. Ця технологія випробувана на перехрестях у кількох містах США. Коли ідентифікується закономірність, поліцейські машини відправляються на перехрестя, де, швидше за все, трапляються аварії в той момент, коли це найімовірніше.

Технологія ШІ привела до 17% скорочення числа аварій на перехресті в штаті Невада. Вказана система ШІ аналізує відеозапис, позначаючи визначені зони та рахує кількість транспортних засобів, які в'їжджають у простір. Також, дані системи Waycare можуть використовуватися для контролю дорожнього руху та уникнення заторів, спричинених автомобільними аваріями[40].

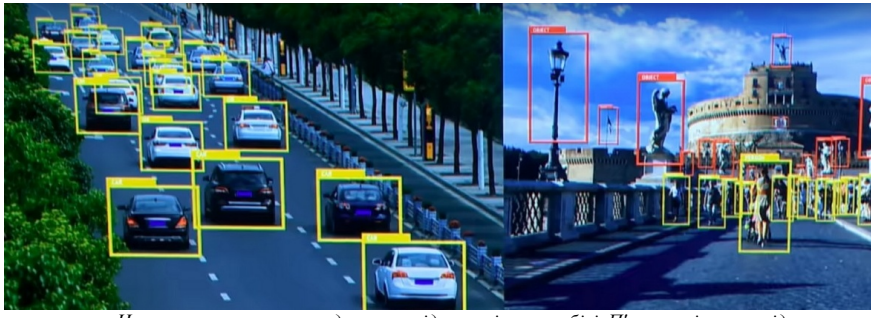
Приклади роботи камери виявлення мобільного телефону за кермом автомобіля в Австралії

В **Австралії** на дорогах встановили камери зі ШІ, вони виявлятимуть водіїв, які користуються телефоном за

[40]Cranenburgh Nadine. How data analysis and AI could help engineers make our roads safer. October 22, 2019. URL: https://createdigital.org.au/engineers-investigating-video-analysis-ai-prevent-road-deaths/

кермом. Система складається з двох пристроїв спостереження: один фіксує номерний знак автомобіля, а інший одночасно визначає положення рук водія, фіксуючи завдяки технологіям ШІ протиправне використання водіями телефонів. Камери можуть працювати в будь-яких погодних умовах, включаючи туман і сильний дощ. Також камери можуть фіксувати номери автомобілів та водіїв за кермом, які порушують правила, перевищуючи швидкість і при наступному порушенні водій отримуватиме штраф. Таким чином, ШІ розшифровує зображення і відокремлює від загальної кількості знімків, ті на яких виявлено водіїв, що користуються мобільним телефоном під час руху автомобіля і надсилає на розгляд відповідних підрозділів правоохоронних органів, які в свою чергу приймають остаточне рішення.

Зазначається, що під час тестування в першій половині 2019 року камери виявили понад 100 тисяч водіїв, які незаконно користувалися телефоном за кермом. У штаті планують до 2023 року встановити 45 таких розумних камер. Застосування різних технологій ШІ за оцінками їх розробників дозволить на 40 % зменшити кількість ДТП[41].



На рисунку жовтими квадратами відзначені автомобілі. П'ять років тому відсоток розпізнавання авто не перевищував 50%, зараз — 100%.

Центр ІТС в Дубаї

У **Об'єднаних Арабських Еміратах (ОАЕ)** *застосування технологій призвело до скорочення на 65% ДТП, викликаних втомою водіїв громадських і приватних транспортних засобів, а загальний рівень безпеки на дорогах збільшився на 83%.*

Передбачено, що до 2023 року всі дороги м. Дубаю (ОАЕ) будуть контролюватися встановленими інтелектуальними транспортними

[41]Mobile Phone Detection Cameras operating in NSW. URL: https://www.mynrma.com.au/cars-and-driving/driver-training-and-licences/resources/mobile-phone-detection-cameras-rolling-out

системами (ІТС). ІТС збирають інформацію про поїздки в реальному часі завдяки чому здатні робити прогнози та пропонувати варіанти для вирішення проблем дорожнього руху.

Безпосереднім ядром роботи зазначеного центру є вузол під назвою I-Traffic, що підключений до численних пристроїв, які відстежують рух, номера автомобілів, швидкість і погоду. Зібрані дані відправляються в центральний вузол, який аналізує їх для складання плану дій або відправки повідомлень водіям.

Всього на дорогах встановлено 245 камер спостереження, які підключені до ІТС. Крім того, встановлено235 пристроїв для моніторингу ДТП і підрахунку транспортних засобів. Це на додаток до 115 пристроїв для обчислення часу в дорозі та швидкості руху, а також 17інформаційних систем, які надають інформацію про погоду, в тому числі про дощ і погану видимість через тумани. Використовуючи дані, зібрані за допомогою цих пристроїв, планується рух в місті під час проведення певних масових заходів або святкувань[42].

Ще одним важливим проектом у цій країні було запровадження системи регулювання та контролю стану водіїв міських автобусів. Кількість аварій, які відбувалися через високий рівень втоми водіїв, скоротилася на 65%.

Важливою розробкою, яка підвищує рівень безпеки пішоходів і водіїв у міському середовищі – дубайська система бронювання місць для паркування. Використовуючи її, водій отримує оптимальне місце для паркування ще до того, як дістанеться до місця паркування.

До введення ІТС кількість аварій не знижувалася нижче 5-8 випадків на день. Після встановлення інтелектуальних камер спостереження на більш, ніж 10 тисячах автобусів й інших одиниць громадського транспорту, загальний рівень безпеки на дорогах збільшився на 83%.

Разом з тим, поліція м. Дубая використовує у професійній діяльності «розумні» окуляри GoogleGlass. За допомогою гаджета поліцейські відстежують порушення автомобілістів, а також отримують сигнали про машини, що знаходяться в розшуку. Поліція ОАЕ вже розробила два власних додатки для GoogleGlass, які будуть використовуватися поліцейськими на службі. Перший додаток дозволяє фотографувати порушення правил дорожнього руху і миттєво передавати інформацію

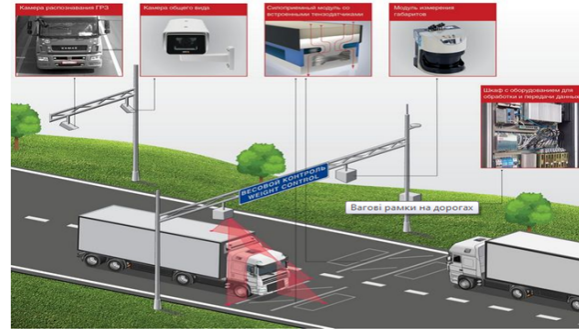
У Китаї поліцейські використовують спеціальні окуляри з вбудованим у них пристроєм розпізнавання осіб.

[42]В Дубаї створили найбільш технологічний в світі ІТС центр. URL:https://pro-mobility.org/2020/12/22/v_dubai_naibilsh_tekhnolohichnyi_v_sviti_its_centr/

в базу даних, інший дозволяє ідентифікувати автомобілі, що знаходяться в розшуку. Для цього працівнику поліції потрібно буде тільки «подивитися» на номерні знаки автомобіля – і GoogleGlass звірить номер з базою даних про викрадені автомобілі, після чого попередить користувача, якщо транспортний засіб знаходиться в розшуку[43].

У **м. Пекіні (КНР)** дорожній патруль протестував першого робота, завданням якого є контроль та виявлення фото або відео фіксація порушень правил дорожнього руху водіями на автостраді. Це невеликий, за розміром, поліцейський автомобіль, що їздить зі швидкістю 5 км/год. Випробування пройшли на автостраді до аеропорту м. Шоуду. Також робот відправляє водіям повідомлення про несприятливі погодні умови, ремонти шляхопроводів або ДТП. При виникненні аварії робот швидко приїжджає на місце, знімає всі необхідні матеріали і відправляє їх до поліції[44].

Німеччина, Австрія, Італія та інші країни. У Німеччині, Австрії, Італії та багатьох інших країнах запроваджено системи зважування вантажних автомобілів в русі (Weight-in-Motion) з метою збирання інформації про дату та час проїзду транспортного засобу, його габаритні розміри, загальну масу та її розподіл по осям. Також фіксуються температура повітря та дорожнього покриття, смуга та напрямок руху, швидкість руху та державний номерний знак. Така система призначена для цілодобового моніторингу руху на автомобільних дорогах і автоматичного виявлення фактів порушення чинного законодавства в сфері вантажних перевезень, не вимагає присутності персоналу та зупинки транспорту.



Автоматизована система вагового контролю

Система вагового контролю такого типу дозволяє:

– забезпечити збереження автомобільних доріг;

– підвищити безпеку дорожнього руху;

– здійснювати контроль транспортних потоків, що проходять через місто;

– створити доказову базу, що забезпечує невідворотність покарання власників транспортних засобів з наднормативними ваговими параметрами;

– отримати достовірну ситуацію про інтенсивність дорожнього руху для планування ремонтно-будівельних робіт.

[43]Поліція Дубая візьме на озброєння окуляри GoogleGlass. URL : https://www.digger.ru/news/policiya-dubaya-vozmet-na-vooruzhenie-ochki-googleglass

[44]Штучний інтелект і робототехніка на службі поліції. URL: https://matrix-info.com/shtuchnyj-intelekt-irobototehnika-na-sluzhbi-politsiyi/

2.1.2. Національний досвід

У **м. Вінниця** на сьогодні вже впроваджена система автоматичного розпізнавання номерів та типу автомобілів. У роботу Ситуаційного центру ГУНП та підрозділів вінницької поліції запроваджується безпековий проєкт «Vezha», в основі якого лежить використання нейронових мереж та ШІ аналітики відеопотоку з понад 600 камер відеоспостереження, які працюють як на вулицях, так і всередині комунальних закладів: зокрема в школах та «Прозорих офісах». Особливу увагу приділяють в'їздам та виїздам з міста, а також центральним вулицям, парковим зонам та вокзалам. При цьому система містить 15 модулів відеоаналітики, які дозволяють автоматично розпізнавати обличчя, номерів та тип автомобіля, відслідковувати людей за різними параметрами[45].

Робота ШІ допомагає працівникам Ситуаційного центру максимально швидко збирає дані про автомобілі, що рухаються міськими дорогами полягає в тому, що камери та програмне забезпечення майже зі 100% точністю розпізнає номер автомобіля, його марку, модель та кольори, в які пофарбоване авто у відсотковому співвідношенні (наприклад 56% – чорний колір, 44% – сірий), що значно спрощує та пришвидшує пошук того чи іншого авто.

Приклад роботи системи ШІ щодо захисту встановленого периметра території

У м. Вінниця таким чином за рік виявили близько 13 тисяч адміністративних правопорушень правил дорожнього руху та правил благоустрою. Ситуаційний центр надав понад 400 відеозаписів на вимогу судів. Як наслідок, з близько мільйона гривень збитків, які виявив Ситуаційний центр, 750 тисяч вже відшкодовано в бюджет.

[45]Вінницька поліція презентувала перший в Україні іноваційний безпековий ІТ-проєкт, який впроваджуватиме в свою діяльність. Офіційний сайт Національної поліції України. URL: https://vn.npu.gov.ua/news/policziya-i-suspilstvo/vinniczka-policziya-prezentuvala-pershij-v-ukrajini-inovaczijnij-bezpekovij-It-projekt-yakij-vprovadzhuvatime-v-svoyu-diyalnist/?fbclid=IwAR3J4ZgKx7DiGAB51fphCI39cJ-gv-N-5RBLQnIDF__h1Zt88yNhY3vT6JU

Управління патрульної поліції другий рік поспіль посідає перше місце в Україні за виявленням автомобілів та водіїв, які зникли з місця ДТП. Відсоток знайдених учасників ДТП складає 94%.

Також, ефективно така система може працювати в контексті боротьби з неправильним паркуванням. Тобто камера може «поставити на охорону» зони, де паркування заборонено, і якщо на це місце стає автомобіль та перебував там понад 5 хвилин (система сама вирахує час) – туди виїжджають патрульні та штрафують недобросовісного водія.

У **м. Маріуполі** поліція використовувала у своїй роботі можливості унікального Єдиного аналітичного сервісного центру, в основу якого покладено новітні технології ШІ та МН. Система, яка базується на аналітичній платформі ULA, здійснює моніторинг оперативної ситуацію у регіоні. Поліція обробляє сигнали, отримані від інтелектуальної відеоаналітики та мобільних додатків, щоб реагувати на ситуацію у режимі реального часу, та відправляти на місце події наряди, які знаходяться найближче.

Центр відеоаналітики в м. Маріуполь, Донецької області.

Новітній Центр базується на системі інтелектуальної відеоаналітики, яка використовує понад 200 камер, встановлених на території усієї області. *За результатом апробації новітньої технології, було доведено, що у 2021 році*

відеоаналітика допомогла встановити близько 800 автомобілів, які перебували у розшуку[46].

Таким чином використання поліцією технологій ШІ на автошляхах надасть можливість:

- підраховувати в автоматичному режимі кількість транспортних засобів за напрямками руху зокрема за умови змінного дорожнього покриття, відсутності маркування, погодних умов, часу доби, тощо впродовж 24 годин 365 днів на рік. Зокрема, забезпечувати підрахунок транспорту у «заторі», «тягучці», під час проїзду розмежувальної лінії чи у разі відсутності такої лінії, наявності великої кількості транспорту, одночасних напрямків руху (до сорока на одній камері включно), тощо. Припустима помилка: <5%;
- виявляти та характеризувати автомобілі за ключовими характеристиками (марка автомобіля, модель автомобіля, покоління автомобіля, колір кузова автомобіля, проміжок часу, адреса, джерело даних) (припустима помилка: <10%);
- розрізняти громадський транспорт (насамперед, тролейбуси та автобуси, які належать до муніципального транспорту) та автоматично давати необхідну команду апаратному комплексу, який контролює перемикання кольору на світлофорному об'єкті;

Кількість відеокамер з можливістю розпізнання номерного знаку по регіонах України.

- забезпечувати можливість перегляду отриманих даних і пошуку за зазначеними параметрами, зокрема: перегляд та експорт таблиці зі всіма визначеними характеристиками, зазначенням часу і місця фіксації, посиланнями на файл-джерело з відео (короткий відеоролик, що включає 10 секунд до і після моменту фіксації), до таблиці додається фото об'єкта;
- забезпечувати можливість керування завданнями обробки даних, їх перегляду та аналізу, формування необхідних аналітичних звітів, таблиць, графічних ілюстрацій, тощо;
- аналізувати відеопотоки з різних типів камер за їхніми якісними характеристиками (локація, кут огляду, тип картинки, розмір картинки, кількість

[46]Аналитическая система ULA в работе полиции. URL: https://ula.lantec.ua/ru/news/analitichna-sistema-ula-u-roboti-politsiji-2

кадрів за секунду часу, тип потоку передавання кадрів тощо), а також, надавати можливість змінювати потоки або додавати нові потоки, камери, локації, тощо без необхідності виїзду на місце представника, змінювати налаштування модулю, його характеристики тощо;

- виявлення та надання характеристики транспортного засобу за такими даними, як марка автомобіля, модель та покоління, колір кузова машини, проміжок часу, адреса реєстрації тощо[47].

47Трафіком в Києві управлятиме штучний інтелект. URL: https://autokyiv.info/2020/10/16/trafikom-v-kyyevi-upravlyatyme-shtuchnyj-intelekt/?fbclid=IwAR1EYctfGknX6WWEwUDkQLiPpbtJVTGygOvHHf_mn7Vkd1l0iinlMUGaEds

2.2. Використання технологій штучного інтелекту у сфері забезпечення публічної безпеки

Важливою сферою суспільного життя є забезпечення охорони прав і свобод людини, протидія злочинності, підтримання публічної безпеки і порядку. Проблемним питанням для правоохоронних органів залишається спостереження за великою кількістю осіб на предмет виявлення потенційних загроз, а тому розробляються технології, які допомагають правоохоронним органам краще виконувати свої обов'язки і забезпечувати громадську безпеку.

Беручи до уваги те, що кримінальні правопорушення не є випадковими, та базуються на конкретних закономірностях, звичайній діяльності, а також на раціональному прийнятті рішень, технології ШІ посилюють найважливіші аспекти роботи поліції у тому числі й в сфері забезпечення публічної безпеки і порядку. Використання технологій ШІ може допомогти у забезпеченні публічної безпеки та порядку Національною поліцією України за наступними напрямками.

2.2.1. Розпізнавання зразків

Одне з домінуючих застосувань МН в поліцейській діяльності. Розпізнавання зразків – це процес розпізнавання закономірностей у даних за допомогою алгоритму машинного навчання.

В основі процесу лежить класифікація подій на основі статистичної інформації, історичних даних або пам'яті самої системи. Тобто, розпізнавання ШІ полягає в використанні МН та когнітивних технології, щоб ідентифікувати та класифікувати неструктуровані дані за конкретними класифікаціями. Ці неструктуровані дані можуть бути зображеннями, відео, текстом або навіть кількісними даними[48].

Розпізнавання зразків відбувається в два етапи. Спочатку йде дослідницька частина. Алгоритм здійснює пошук шаблонів загалом. Після йде описова частина,

[48]Understanding The Recognition Pattern Of AI. URL: https://www.forbes.com/sites/cognitiveworld/2020/05/09/understanding-the-recognition-pattern-of-ai/?sh=a02608221c7a

де алгоритм починає класифікувати знайдені закономірності. Поєднання обох цих способів використовується для отримання висновків.

Методи розпізнавання зразків корисні для вирішення проблем класифікації, виявлення шахрайства або розпізнавання зразків для криміналістики, наприклад, для порівняння відбитків пальців[49].

Кримінальні правопорушення можуть бути пов'язані між собою і можуть здійснюватися однією і тією ж особою (особами), або можуть застосовуватися однакові способи дії. Таким чином, значно підвищити ефективність своєї діяльності, правоохоронні органи якщо зможуть виявити закономірності вчинення кримінальних правопорушень. Дані, які поліція отримує від повідомлення про кримінальні правопорушення, є по суті неструктурованими даними. Ці дані необхідно впорядкувати та «просіяти», щоб знайти закономірності.

Машинне навчання є дієвим інструментом під час виконання таких завдань. Інструменти машинного навчання можуть швидко порівнювати різні кримінальні правопорушення та створювати оцінку подібностей. Згодом, ці оцінки можуть бути використані програмним забезпеченням, щоб встановлювати, чи існують загальні закономірності. Система розпізнавання зразків, може бути корисною під час коли потрібно:

- визначити знайомий шаблон швидко і точно;
- класифікувати незнайомі об'єкти;
- розпізнати фігури та предмети з різних сторін;
- розкрити візерунки та предмети, навіть частково приховані;
- автоматично розпізнавати шаблони[50].

2.2.2. Прогностична аналітика

Прогностична аналітика – це ефективне застосування машинного навчання. Інструмент, який має функції прогнозуючої аналітики, використовує машинне навчання, щоб допомогти правоохоронним органам в покращенні забезпечення громадської безпеки. Вони зосереджені на визначення тенденцій злочинності загалом. Коли такі тенденції помічені, поліція може активно вживати заходів для попередження та профілактики кримінальних правопорушень.

Такі системи сприяють підвищенню ефективності роботи Національної поліції та допоможуть в їх роботі. Використовуючи інструмент прогнозної аналітики, поліції може отримувати інформацію щодо стану злочинності певної місцевості або області та визначати її тенденції. Це дасть змогу під час патрулювання працівниками поліції раціонально розподілити ресурси в певній області, щоб активно керувати ситуацією та запобігати вчиненню протиправних дій.

Очевидний вплив розумних рішень із використання систем ШІ у відеоаналітиці під час організації громадської безпеки. Все більше і більше

[49]Blog: Pattern Recognition. URL: https://serokell.io/blog/pattern-recognition.
[50]Blog: Pattern Recognition. URL: https://serokell.io/blog/pattern-recognition.

правоохоронних органів у всьому світі використовують відеоспостереження, щоб розширити свої можливості.

Hi-tech лабораторія в Великій Британії, де поліцейські застосовують-технології штучного інтелекту для розслідування кримінальних правопорушень.

Відеоаналітика МН на основі ШІ може стати важливим розвитком у правоохоронних органах у найближчі роки[51]. Ці системи використовують широкий спектр датчиків для збору відео та даних й здатні не лише записувати всі події у секторі спостереження, а й відокремлювати інформацію із загального відеопотоку, аналізувати та структурувати її за визначеними у програмі критеріями. За даними Інтерполу і Європолу, більш ніж в 70 країнах поліцейські на практиці використовують ті чи інші види предиктивної аналітики.

Hi-tech лабораторія в Великій Британії, де поліцейські застосовують-технології штучного інтелекту для розслідування кримінальних правопорушень.

[51]Скотленд-Ярд вооружился искусственным интеллектом. URL: https://www.kommersant.ru/doc/4081359

Системи відеоспостереження видають величезну кількість відео. Через брак часу чи ресурсів більшість цього відео ніколи не переглядається. Як результат, інциденти безпеки пропускаються, і підозріла поведінка не виявляється вчасно, щоб запобігти правопорушенням. Ці проблеми, сприяли розвитку відеоаналітики.

Відеоаналітика автоматично генерує описи того, що відбувається у відео із камер спостереження, які можна використовувати для відстеження людей, автомобілів та інших об'єктів, виявлених у відеопотоці, а також їх зовнішнього вигляду та рухів. Потім цю інформацію можна використовувати як основу для повідомлення центру оперативного реагування правоохоронних органів.

Технології відео нагляду використовують для:

– *Ідентифікація особи правопорушника.* Технології глибокого навчання, вбудовані в системи відеоаналітики, допомагають знаходити деталі, які не можна розпізнати під час людського візуального огляду. Ці системи можуть розрізняти людей за статтю, розміром, швидкістю ходьби та іншими тонкими факторами. Система також може відфільтрувати людей за кольором їхньої сукні або знайти лише пішоходів, які несуть рюкзаки. Наприклад, якщо слідчому необхідно розшукати особу підозрюваного, та попередньо відомо що це є чоловік, одягнений в білу сорочку і з рюкзаком, відеоаналітика на основі ШІ дозволяє йому зосередитись лише на людях, які відповідають опису, виключаючи інших із каналу відеопотоку.

Як тільки розшукувана особа буде ідентифікований як така що відповідає опису, система може знайти цю саму особу в інших відеопотоках та сегментах. Ізолювати цю особу та простежити її пересування.

Приклад роботи аналітики на основі ШІ щодо встановлення особи підозрюваного

– *Визначення місця вчинення кримінального правопорушення.* Пошук місць, де здійснюється правопорушення, наприклад, таких, що вимагають від правоохоронних органів постійного спостереження за мікрорайонами міста, певними відрізками вулиць протягом декількох днів. Таке спостереження може

бути особливо актуальним на тлі постійно зростаючої кількості купівлі-продажу наркотичних засобів безконтактним способом. Саме цей процес можна в значній мірі автоматизувати, розмістивши камеру спостереження та забезпечивши, щоб система аналітики стежила за пішим трафіком з метою виявлення, наприклад, можливого місця закладки як наркотичних засобів чи психотропних речовин, так і самих закладників. Якщо між одним пунктом до іншого певного місця вулиці, території парку, і т. д., підозріло пересувається особа чи декілька осіб, система фіксує та визначає це місце, яке ймовірно є місцем, де приховуються чи знаходяться наркотичні засоби,психотропні речовини чи прекурсори.

– *Критична реакція на інцидент.* Оцінка величини натовпу та підрахунок потоку транспортних засобів та пішохідного руху в районі зазвичай є дуже трудомістким завданням. Система відеоаналітики забезпечує доступні для захисту міри, які дозволяють поліції краще розподіляти ресурси для контролю ситуацій для забезпечення публічної безпеки та правопорядку. Ці аналізи можна проводити в режимі реального часу або базуватись на заархівованому відео. В свою чергу, це сприяє правильному використанню ресурсів підрозділами правоохоронних органів.

Отже, відеоаналітика (VideoAnalytics)– це комп'ютеризований аналіз відеозаписів, який використовує алгоритми для розмежування типів об'єктів та виявлення певної поведінки чи дій у режимі реального часу, забезпечуючи попередження та уявлення користувачам.

Так, з метою вирішення завдань, які стоять перед правоохоронними органами, закордонні компанії, що займаються охороною громадського порядку, поєднують системи відеоспостереження із системами ШІ. Ці системи підтвердили свою ефективність у боротьбі зі злочинністю та забезпеченні безпеки населення.

2.2.3. Міжнародний досвід

В **м. Лос-Анджелес (США)** поліція співпрацює з компанією «PredPol». В основі цієї системи є алгоритм що, визначає потенційні місця учинення протиправних діянь. Під час експериментального випробовування було встановлю результативність PredPol, яка є мінімум у два рази більшою за традиційні підходи, що застосовуються поліцейськими у їх повсякденній професійній діяльності.

Зокрема, розкриття правопорушень після застосування вказаної технології підвищується від 10% до 50%. Щодо окремих видів правопорушень, то застосування прогнозної поліцейської діяльності дозволяє скорочувати рівень грабежів до 50%, а крадіжок, поєднаних із проникненням у житло, – до 70%[52].

В **м. Нью-Йорк (США)** у 2007 р. був створений централізований операційний центр громадської безпеки. Здійснено інтеграцію понад сто розрізнених джерел даних. Усі потоки інформації від патрульних машин, безліч камер відеоспостереження, у вигляді неструктурованих даних перетворюються на

[52] Smith Mark. Can we predict when and where a crime will take place?30 October, 2018. URL: https://www.bbc.com/news/business-46017239

універсальний формат. Потім аналітичні інструменти ШІ асоціюють інформацію, поміщаючи її у певний контекст, та розподіляють її відповідно до запитів користувачів. Аналітична система асоціювання розпізнає як структуру, а й значення інформації, включаючи взаємини між різними частинами. *Створення єдиного сховища дозволило знизити злочинність у місті на 27%.*

В **м. Чикаго (США)** поліція протестувала комбінацію з найновіших технологій і підходів, щоб знизити рівень злочинності. Система ШІ, що працює на основі потокового відео, BigDate і МН на основі записів потокового відео з відеокамер, контролює шість районів міста. Таким чином, вона передбачає злочини, допомагає поліції встановлювати особу порушника і може автоматично надіслати до небезпечного місця підрозділ оперативного реагування. Так, один із інструментів – Hunch Lab – об'єднує статистику злочинності з соціально-економічними даними, щоб визначити, де може статися злочин.

Обладнання ShotSpotter на основі ШІ, що працює на перехресті Саут-Стоні-Айленд в Чикаго

В результаті лише в одному із шести районів міста, в якому випробовувалась технологія, за допомогою прогнозів штучного інтелекту впродовж 7 місяців вдалося попередити значну кількість кримінальних правопорушень, та зменшивши статистику вбивств на 33% порівняно з попереднім роком. Така статистика підтвердилася і в інших районах де показники теж істотно змінилися – на 9-18% зменшилася кількість вбивств.[53]

У **м. Мемфіс (США)** підтвердилася ефективність системи Blue CRUSH (від англ. Crime Reduction Utilizing Statistical History – «зниження злочинності на основі статистичних даних»), розроблений для поліції компанією IBM програмний продукт завдяки ШІ здійснює аналіз наявної статистики вчинення

[53]Штучний інтелект і робототехніка на службі поліції. URL: https://matrix-info.com/shtuchnyj-intelekt-i-robototehnika-na-sluzhbi-politsiyi/

кримінальних правопорушень за значний період та визначає самостійно місця потенційної загрози майбутніх кримінальних правопорушень(у межах кількох кварталів) та часу (у межах кілька годин конкретного дня тижня). *В результаті використання системи Blue CRUSH в діяльності поліції призвело до зниження рівня злочинності у м. Мемфіс на 31%, у тому числі 15% є тяжкі кримінальні правопорушення.*

У **м. Ванкувер (Канада)** поліція впровадила систему аналізу даних, засновану на розробках IBM та географічній інформаційній системі Esri. Система не тільки виявляла тенденції, а й передбачала ймовірний час та місце вчинення кримінальних правопорушень. *З 2007 по 2011 роки кількість кримінальних правопорушень, пов'язаних із власністю, скоротилася на 24%, а насильницькі кримінальні правопорушення – на 9%.*

У **м. Кент** (**Велика Британія)** технологія прогнозування PredPol та системи Geolitica в дозволило скоротити вуличне насильство *на 6% лиши протягом чотирьох місяців*[54].

У **м. Тренто** (**Італія)** з листопада 2012 року по травень 2015 року відбулася реалізація проєкту «Електронна безпека – інформаційні та комунікаційні технології засновані на знаннях і прогнозувані міської безпеки». Його мета була спрямування роботу правоохоронних органів на попередження злочинності та підвищення безпеки в містах. В рамках проєкту було використано базу даних, що збирає інформацію про кримінальні правопорушення, та доведення її до відома поліції. *В результаті випробовування була підтверджена надійність використовуваних методів, які дозволяють прогнозувати протиправні діяння з коефіцієнтом успішності близько 60–65% і які сприяють підвищенню ефективності боротьби зі злочинністю при наявності обмежених ресурсів.*

У **Ірландії** технологія ШІ Kinesense виявляє підозрілу поведінку на зображеннях з камер відеоспостереження в режимі реального часу чим звільняє співробітників поліції від перевантажень, відбираючи відео, що містить необхідну інформацію для розслідування справ.

У **Німеччині** в діяльності поліції планують використовувати програмне забезпечення на основі ШІ яке здатне попереджати про вчинення кримінального правопорушення. Проект називається Precobs. Програма, розроблена німецькою компанією, прогнозує найбільшу ймовірність вчинення кримінального правопорушення, його місце і час.

2.2.4. Національний досвід

У**м. Вінниці** практичне використання впровадження систем відеоаналітики в Україні застосовують у Вінницькій обл. Головне управління Національної поліції у Вінницькій області вперше в Україні запровадило у свою роботу безпековий проєкт «Vezha», в основі якого лежить використання ШІ аналітики

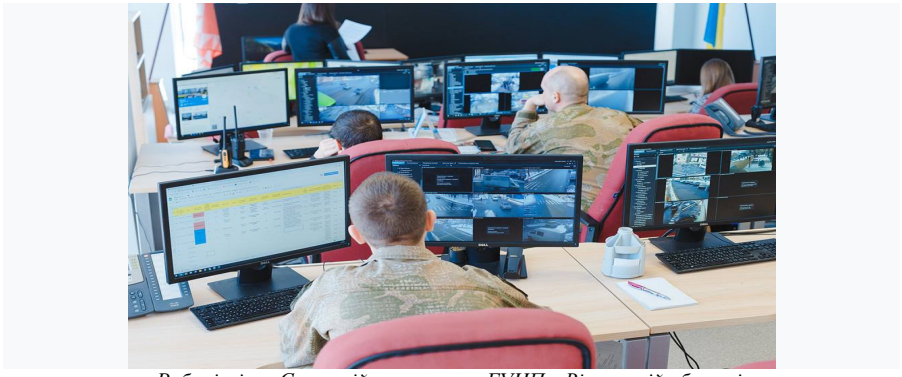
[54] Smith Mark. Can we predict when and where a crime will take place? URL: https://www.bbc.com/news/business-46017239

відеопотоку з камер відеоспостереження. Розробником програмного забезпечення виступила компанія «Incoresoft Україна» з Вінниці.

Використання такого програмного забезпечення має на меті консолідувати зусилля сторін на співпрацю в частині попередження та недопущення порушень публічної безпеки та порядку, підвищення ефективності протидії злочинності та захисту прав громадян шляхом впровадження системи «Vezha» на основі ШІ і нейронних мереж в роботу ситуаційного центру ГУНП та підрозділів вінницької поліції.

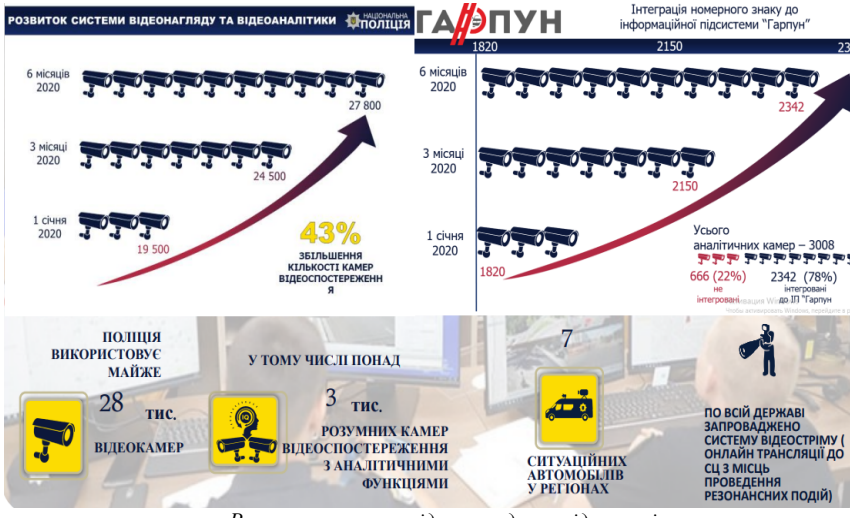
Система «Vezha» спрямована на безпеку міст і використовує 15 модулів відеоаналітики, що в свою чергу дозволить розпізнавати об'єкти, номерні знаки, обличчя та відслідковувати людей за різними параметрами. на основі ШІ. Це в сотні разів прискорить процес отримання, обробки та зберігання даних, користуватися якими зможе кожний поліцейський у своїй роботі задля успішного створення безпекового середовища в місті та області. Система пришвидшить розкриття кримінальних правопорушень, реагування на них та пошук зниклих людей, зокрема, дітей. Впровадження цієї системи дозволить поліції якісніше виконувати свої функції та забезпечувати громадську безпеку та порядок в місті[55].

[55] Вінницька поліція впровадила систему відеоспостереження «Vezha» на основі штучного інтелекту і нейронних мереж. URL: https://itc.ua/news/vinniczka-policziya-vprovadila-sistemu-videosposterezhennya-vezha-na-osnovi-shtuchnogo-intelektu-i-nejronnih-merezh/



Робочі місця Ситуаційного центру ГУНП у Вінницькій області.

У **м. Маріуполь** поліція продемонструвала роботу унікального Єдиного аналітичного сервісного центру, в основу якого покладено новітні технології ШІ та МН. Система, яка базується на аналітичній платформі, допомагає моніторити оперативну ситуацію у регіоні. Поліція обробляє сигнали отримані від інтелектуальної відеоаналітики та мобільних додатків, щоб реагувати на ситуацію у режимі реального часу, та відправляти на місце події наряди, які знаходяться найближче[56].



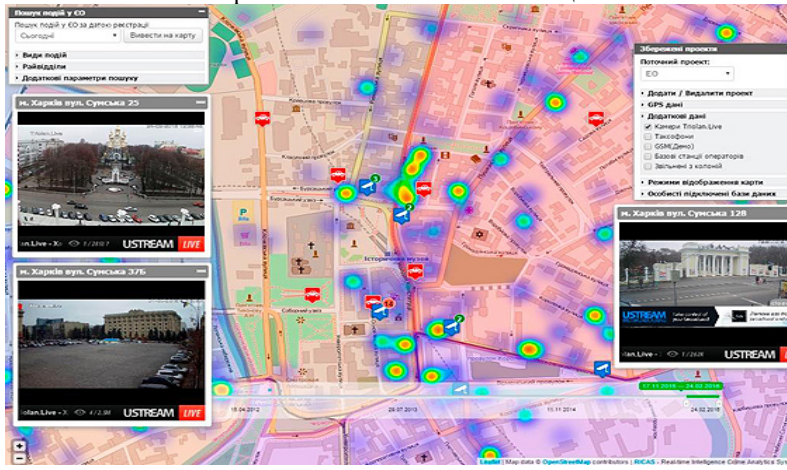
Розвиток системи відеонагляду та відеоаналітики

[56]Аналітична система ULA у роботі поліції. URL: https://ula.lantec.ua/news/analitichna-sistema-ula-u-roboti-politsiji

Правоохоронна діяльність, керована аналітикою, дозволяє бачити ширшу картину, визначаючи тенденції та зразки (почерк), шляхом пов'язування між собою кримінальні правопорушення, об'єктів, осіб, ознак, місця через проведення кримінального аналізу. Інформація, що надходить від громади, – одна з найважливіших складових роботи правоохоронних органів, керованої аналітикою, як і в моделі взаємодії поліції з громадами (community policing). Насправді ж обидві згадані моделі роботи поліції не можуть належним чином функціонувати одна без одної.

Типи кримінальних правопорушень, як правило, скупчуються у просторі та часі, а дані, пов'язані із злочинністю, такі як вид, місце кримінального правопорушення, зброя, за допомогою якої вчинялося діяння, можуть допомогти передбачити майбутні місця кримінальних правопорушень. Наприклад, розкрадання крадіжок в одній області може допомогти передбачити, що подібні випадки можуть траплятися в прилеглих районах у майбутньому. Таким чином, системи ШІ можуть допомогти працівникам міліції визначити місце розташування районів, де їм слід розглянути питання посиленого патрулювання.

У **м. Харків** було запущено програмно-апаратний комплекс аналітичного супроводу оперативно-розшукової діяльності та підтримки прийняття рішень (Ricas), який було розроблено співробітниками Управління інформаційного забезпечення ГУ НПУ в Харківській області спільно з місцевими ІТ-компаніями.



Система є надбудовою над існуючими інформаційними системами НП України. Головною особливістю системи є візуалізація на географічній карті інформації НП України з її подальшим аналізом. Фактично це геоінформаційна аналітична система НП України. Система «RICAS» дозволяє аналітику виконувати такі види кримінального аналізу інформації:

- аналіз кримінальної обстановки;
- аналіз загального профілю;
- аналіз конкретного кримінального провадження;
- порівняльний аналіз;

- аналіз кримінальних правопорушень вчинених організованою групою;
- аналіз особливостей профілю;
- аналіз розслідувань кримінальних проваджень.

Інструментарій системи «RICAS» базується на математичних моделях і методах інтелектуального семантичного аналізу, візуального темпорального аналізу, аналізу поведінкового профілю, аналізу прихованих закономірностей

Можливість відображення на карті рухомих об'єктів дозволяє відстежувати ситуацію в динаміці, і, відповідно, забезпечувати адекватну і своєчасну реакцію

Система дозволяє виявити логічні відкриті та приховані зв'язки між заданими об'єктами і відобразити їх як у вигляді геоінформації, так і з використанням числового ряду.

Відображення на інтерактивній карті підключених камер і можливість миттєвого доступу до кожної з них як в режимі потокового відео, так і в режимі запису дозволяє відслідковувати як саму подію, так і дії служб реагування, фіксувати обставини правопорушення і у разі потреби використовувати дані в якості доказової бази в ході слідства[57].

З появою аналітики великих даних, МН та систем ШІ як оцінка ризику злочинності, підрозділи НП України можуть протистояти сучасним викликам злочинності, таким як:

- попередження правопорушень. Правоохоронні органи зможуть реагувати не лише на випадки правопорушень, але активно працювати над їх попередженням. Завдяки МН з'являється можливість передбачити, де може статися протиправне діяння, і вчасно відреагувати на подію;
- серійні суспільно небезпечні діяння можуть мати свою закономірність, і цю схему потрібно ідентифікувати, щоб розслідувати кримінальне правопорушення. Для правоохоронних органів відстежити велику кількість кримінальних правопорушень, та визначити закономірності не є легкою задачею, тому новітні технології є необхідними у цій сфері.
- визначення місць які більш схильні до вчинення кримінальних правопорушень. Визначення ймовірних таких місць є нелегкою справою. Про те така перспектива передбачити можливі місця, де можуть статися протиправне діяння, і може працювати над попередженням вчинення таких діянь. Також, поліція у своїй діяльності може стикатися з обвинуваченням у дискримінації меншин, етнічних чи релігійних. Тому, завдання, що стоїть перед поліцією, полягає в тому, щоб ефективно виконувати свої обов'язки, не наражаючись із звинуваченнями в дискримінації;
- виявлення небезпечної інформації в мережі Інтернет. В Інтернеті публікується багато картинок, фотографій, відео та ін., які можуть містити інформацію провокативного характеру, чи таку, що підбурює до насильства або вчинення протиправних дій. Завдання поліції полягає в тому, щоб вчасно виявляти й реагувати на таку інформацію в мережі Інтернеті, не порушуючи прав людей.

[57]RICAS - Realtime intelligence crime analytics system. URL: https://ricas.org/uk/#press-about-us

Поширення та стрімкий розвиток інформаційно-телекомунікаційних систем (ІТС) й інформаційно-комунікаційних технологій (ІКТ) сприяли соціальному прогресу, що в свою чергу, змінило спосіб життя людей у певних сферах суспільних відносин. В Україні та в усьому світі щороку вчиняються десятки тисяч кіберзлочинів з використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. З розвитком технологій стрімко зростає кількість кримінальних правопорушень у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті будуть одними з найчисельніших[58].

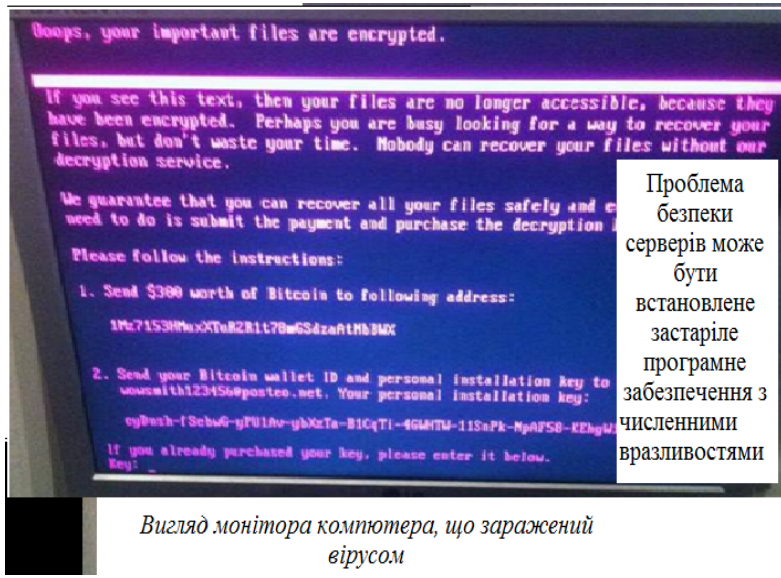
Із таким розвитком світова спільнота отримала не лише переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Так як кібербезекавиступає в якості національної безпеки, очевидно, що забезпечення такої безпеки та злагоди в кіберпросторі стає головним завданням інформаційної епохи. Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам[59].

В цілому складність механізму вчинення конкретного виду кіберзлочину зумовлюється певними чинниками, зокрема: 1) терміном реагування на звернення та повідомлення про кіберзлочини; 2) рівнем кібербезпеки держави; 3) ступенем «комп'ютерної безграмотності» потенційних жертв кримінальних

[58]Нікулеско Дмитро. Кібербезпека: вразливі моменти. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html

[59]Кібервійна. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B2%D1%96%D0%B9%D0%BD%D0%B0#%D0%92%D0%B8%D0%B4%D0%B8_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B2%D1%96%D0%B9%D0%BD%D0%B8

правопорушень; 4) темпами усунення недоліки в роботі правоохоронних органів. На зниження ступеню «комп'ютерної безграмотності» потенційних жертв кримінальних правопорушень впливатиме діяльність Національної поліції з виявлення та прогнозування можливих кіберзагроз, у тому числі з використанням ШІ. Також, важливим в цілях протидії кіберзлочинів є зменшення часу реакції Національної поліції України на вхідну інформацію про кримінальне правопорушення.

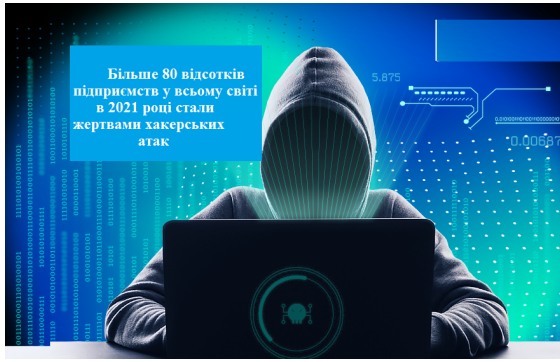


Вигляд монітора компютера, що заражений вірусом

Кібербезпека реалізується через певні організаційні заходи за допомогою технічних методів і засобів, що забезпечують цілісність, доступність, автентичність, а також, за необхідності, конфіденційність інформації під час обміну та доступу до електронних інформаційних ресурсів.

Сучасні кіберзагрози зумовлені спробами несанкціонованого доступу, маніпуляцією, модифікацією та іншими діями над інформацією, які направлені на порушення критеріїв безпеки та може додатково завдати великих фінансових збитків на державному рівні. Програмне забезпечення, яке працює на комп'ютерах та інтелектуальних пристроях, може проявляти вразливі місця в сфері безпеки, які можуть бути використані хакерами. Потенційні наслідки мають великі масштаби і коливаються від безпеки особи до рівня нації чи регіону.

Тому активне використання нових моделей, нових методів та нових технологій для ефективного запобігання та боротьби з різними кримінальними правопорушеннями в галузі Інтернету стало загальним питанням правоохоронних органів.



Для забезпечення захисту від сучасних кіберзагроз їх необхідно ефективно виявляти. В багатьох засобах захисту інформації присутні підсистеми виявлення, які забезпечують вирізнення та ідентифікацію кіберзагроз

Для боротьби з кіберзлочинністю потрібні високотехнологічні засоби. ШІ ідеально підходить для вирішення деяких з найскладніших проблем, і кібербезпека, безумовно, потрапляє в цю категорію. Збільшення кібератак і поширення пристроїв дозволяють використовувати МН і ШІ, автоматизуючи виявлення загроз і реагуючи більш ефективно, ніж традиційні програмні підходи[60].

Останнім часом ШІ відіграє важливу роль у боротьбі з кібератаками та кіберзлочинцями. Рішення та програми безпеки, підтримувані ШІ, створюють інноваційні та невимушені підходи для забезпечення кращої кібербезпеки. Мета ШІ полягає у розумінні, виявленні та припиненні сумнівних дій у системі. Такі атаки можуть охопити різні структури. На практиці кібератаки можуть мати різну форму, проте, найчастіше такі речі пов'язуються як злом чи зловмисне програмне забезпечення, і, можливо, фішинг[61].

[60]Штучний інтелект для захисту вашого бізнесу. URL: https://www.bdo.ua/uk-ua/news-2/2020/artificial-intelligence-to-protect-your-business.

[61]How Artificial Intelligence is helping fend off cyberattacks. URL: https://www.dqindia.com/artificial-intelligence-helping-fend-off-cyberattacks/

Безпека ШІ передбачає використання ШІ для виявлення та зупинки кіберзагроз з меншим втручанням людини, ніж це зазвичай очікується або потрібно за традиційних підходів до безпеки.

Здатність ШІ аналізувати величезні обсяги даних із блискавичною швидкістю означає, що загрози безпеці можуть бути виявлені в режимі реального часу або навіть передбачені на основі моделювання ризиків.

Тому завданням ШІ має бути вдосконалення засобів безпеки, і перш за все, пришвидшення реагування на випадки, як тільки виявляється шкідливе програмне забезпечення щоб не допустити витоку даних. Інструменти безпеки ШІ працюють над виявленням, прогнозуванням, обґрунтуванням, діянням та вивченням потенційних загроз кібербезпеки, не потребуючи особливого втручання людини.

За даними 11-го звіту Cisco з кібербезпеки (Cisco, 2018, Annual Cyber security Report, ACR), щоб скоротити час виявлення зловмисників, фахівці з кібербезпеки починають все більше застосовувати (і закуповувати) засоби, які використовують ШІ і МН[62].

[62]Cisco розповіли, як компанії захищаються від кібератак. URL: http://www.telesphera.net/news/cisco-%D1%80%D0%BE%D0%B7%D0%BF%D0%BE%D0%B2%D1%96%D0%BB%D0%B8,-%D1%8F%D0%BA-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%97-%D0%B7%D0%B0%D1%85%D0%B8%D1%89%D0%B0%D1%8E%D1%82%D1%8C%D1%81%D1%8F-%D0%B2%D1%96%D0%B4-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA.html

ШІ і МН істотно прискорюють реагування на загрози, визнають аналітики Nemertes Research. За їх словами, сьогодні це вже серйозний ринок, сформований під впливом реальної потреби. У Nemertes провели глобальне дослідження, присвячене безпеці, і його результати свідчать: в середньому на виявлення атаки і реагування на неї в організаціях йде 39 днів, проте в деяких компаніях зуміли скоротити цей час до лічених годин. Швидкість реагування безпосередньо залежить від рівня автоматизації, яка забезпечується засобами ШІ і МН. Середній час виявлення атаки – година. У компаніях, які застосовують МН, на виявлення йде менше 10 хвилин, а в тих, що його не використовують – дні або тижні. Що стосується середнього часу аналізу загроз, він становить близько трьох годин. У кращих випадках на такий аналіз йдуть хвилини, в гірших – дні або тижні. Поведінковий аналіз загроз вже застосовується в 21% компаній, які брали участь в опитуванні. Системи виявлення на основі ШІ, як правило, працюють з невизначеністю, вони корисні не лише для попередження, коли щось здається не так, а й для оцінки того, наскільки близька дана подія від кібератаки.

Звіт за результатами міжнародної спецоперації Національної поліції України з правоохоронними органами Сполучених Штатів Америки та Австралії.

ШІ має можливість ефективно аналізувати та повідомляти одночасно про велику кількість кіберзагроз набагато швидше, ніж це могла б зробити людина. АІ вдосконалюється в міру зростання обсягу отримуваних даних. При накопиченні досить великих зрізів даних системи здатні виявляти дуже ранні ознаки появи нових загроз Тому використання ШІ та МН для виявлення вразливостей значно покращує людські можливості.

ШІ може стати «розумнішим» і «вчитися;» оскільки алгоритм ШІ продовжує пошук та моніторинг даних, він може покращити своє розуміння різних типів потенційних атак.

Згідно з дослідженням, проведеним PwC та Радою з питань захисту даних під назвою «Інтернет-ринок кібербезпеки: що криється внизу», ШІ та МН будуть забезпечувати «кімнати кібервійни» в організаціях, щоб допомогти їм захиститися від збільшення кібератак, а також виявляти, прогнозувати і реагувати на те саме.

Програми захисту ШІ можуть аналізувати величезний обсяг інформації та допомагати збирати пов'язані дії, які можуть свідчити про підозрілу поведінку. До загальних можливостей засобів захисту ШІ належать:

- «навчання» на основі минулої поведінки для швидкого, ефективного контексту та розуміння, коли представлено нову або невідому інформацію / поведінку;
- роблячи логічні, виведені висновки на основі потенційних неповних підмножин даних;
- представлення кількох рішень відомої проблеми, щоб надати командам безпеки можливість вибрати найкращий шлях до виправлення.

Методи завдяки яким ШІ може забезпечити кращу кібербезпеку.

1. Оновлення бази даних та розпізнавання загроз. ШІ є важливим фактором, який дозволяє оновлювати бази даних з міркувань безпеки. ШІ збирає різноманітні дані з різних записів та каталогів. Зібрані дані будуть подальшим аналізом для розпізнавання загроз. Ці загрози або небезпеки доставляються кіберзлочинцями ШІ здатний розпізнавати тенденції шпигунського, шкідливого програмного забезпечення та вірусів, і для цього він повинен аналізувати дані з кількох каналів. ШІ може ідентифікувати загрози швидше і попереджати нанесення будь-якої шкоди ..

2. Визнати нехарактерну дію. ШІ дозволяє виявляти ненормальну активність у системі. Він здатний перевіряти нехарактерні дії або ненормальну активність, збираючи адекватний обсяг даних шляхом постійного сканування системи. ШІ також виявляє випадки несанкціонованого доступу. Щоразу, коли виявляється якась нехарактерна дія, ШІ використовує конкретні фактори, щоб перевірити, чи означає це реальну небезпеку, чи це просто підроблена тривога. Щоб ШІ вирішив, що таке ненормальна діяльність, а що ні, потрібна допомога МН. МН також розвивається з часом, що ще більше дозволить ШІ виявляти навіть незначні відхилення. Отже, ШІ має змогу вказувати на все помилково запущене в системі.

3. Виявлення недоліків. ШІ допомагає виявити переповнення даних у буфері. Іноді програми використовують додаткові дані, ніж зазвичай, що

називається переповненням буфера. Крім помилки, допущеної людськими ініціаторами, порушення ключових даних. Ці ковзання також виявляються ШІ, це теж в часі, що дозволяє уникнути подальших ризиків. За допомогою МН штучний інтелект може точно знаходити помилки, пов'язані з кібербезпекою, помилками та іншими недоліками. МН надалі допомагає ШІ виявляти підозрілі дані, що надсилаються із будь-якої програми. Вірус або шкідливе програмне забезпечення, яке використовує хакер для отримання доступу до систем та викрадення даних, здійснюється через вразливості мов програмування.

4. Запобігання загрозам. Розробники ШІ в сфері кібербезпеки регулярно розробляють технології, які попередній формі повинні виявити загрозу в системі або навіть в оновленні. Подальше буде автоматично відвертати будь-кого, щоб використати ці недоліки. ШІ слугував би вражаючою технікою, щоб уникнути будь-якої загрози. Він може вставити додаткові брандмауери разом із виправленням помилок кодування, що значно опереджає ризикам виникнення кібератак.

5. Реагування на загрози. Це те, що відбувається на наступному етапі, тобто коли загроза потрапляє всередину системи. Як обговорювалося вище, ШІ застосовується для виявлення нехарактерних дій та побудови структури вірусів чи шкідливих програм. Зараз ШІ робить відповідний крок проти вірусу чи шкідливого програмного забезпечення. Реакція, в основному, полягає у позбавленні від вірусу, усуненні недоліків та компенсації заподіяної шкоди. І нарешті, ШІ гарантує, що такий інцидент не повториться, і вживає відповідних заходів для запобігання цьому[63].

Звичайний підхід для виявлення та запобігання кібератакам покладається на певне програмне забезпечення, брандмауер, антивірус та подібні інші інструменти. Це вимагає регулярного оновлення системи та програмного забезпечення. Окрім цього, воно вимагає людського втручання, наприклад, вирішення інтенсивності безпеки відповідно до веб-сайту або будь-якої віртуальної платформи.

ШІ здатний перевершити периметри людського інтелекту. Він створений для суворого контролю за можливостями будь-яких кіберзагроз у будь-який момент часу. З розвитком новаторських технологій, таких як МН, підтримка, отримана ШІ, величезна. ШІ успішно заважає кіберзловмисникам отримати доступ до систем або серверів, що зберігають безцінні дані та інформацію

Окрім вищезазначених пунктів, ШІ допомагає забезпечити віртуальний простір багатьма іншими способами. Постачальники кібербезпеки користуються можливостями ШІ та МН, щоб захистити більшість продуктів та програм. Ці нові технології, що передбачають глибоке навчання, також зміцнюють системи безпеки. Засоби захисту ШІ за своєю суттю здатні корелювати події та реагувати на них, що значно скорочує час, необхідний для реагування на події та виправлення. 64% респондентів стверджують, що ШІ знижує витрати на

[63]How AI Can Ensure Better Cyber Security? URL: https://www.innefu.com/blog/how-ai-can-ensure-better-cyber-security

виявлення порушень та реагування на них та зменшує загальний час, необхідний для виявлення загроз та порушень, до 12%[64].

Позитивне використанням впровадження ШІ в галузі кібербезпеки є запровадження біометричних логінів. Біометричні логіни все частіше використовуються для створення захищених входів шляхом сканування відбитків пальців, сітківки або відбитків долонь. Це можна використовувати окремо або разом із паролем, і воно вже використовується в більшості нових смартфонів. Великі компанії стали жертвами порушень безпеки, які ставили під загрозу адреси електронної пошти, особисту інформацію та паролі. Експерти з кібербезпеки неодноразово повторювали, що паролі надзвичайно вразливі до атак Cuber, порушуючи особисту інформацію, дані кредитної картки та номери соціального страхування. Це все причини, чому біометричні логіни є позитивним внеском ШІ у кібербезпеку. ШІ також може використовуватися для виявлення загроз та інших потенційно шкідливих дій. Звичайні системи просто не можуть встигати за великою кількістю шкідливих програм, які створюються щомісяця, тому це потенційна сфера для втручання ШІ та вирішення цієї проблеми. Компанії з кібербезпеки навчають системи ШІ виявляти віруси та шкідливі програми за допомогою складних алгоритмів, щоб потім ШІ міг запускати розпізнавання шаблонів у програмному забезпеченні.

Системи ШІ можна навчити виявляти навіть найменшу поведінку атак-викупників та шкідливих програм, перш ніж вони потраплять до системи, а потім ізолювати їх від цієї системи. Вони також можуть використовувати передбачувані функції, які перевершують швидкість традиційних підходів[65].

Технології ШІ впроваджуються, серед іншого, для захисту даних у хмарних сховищах, класифікації DDoS-атак та їх виявлення. Хмарні сховища вже давно працюють на чолі найбільш значущих технологій, які домінують у середовищі управління даними, полегшуючи все: від розгортання великих даних до прогнозуючої аналітики, від додатків когнітивних обчислень до додатків граничних обчислень. Тому, коли дані мають вирішальне значення, а одне з ключових завдань – захистити їх, хмарні сервіси найкраще підходять для забезпечення як зберігання та обробки інформації, так і для її безпеки. Крім того, масштабність хмарних сховищ якраз підходить для характерних додатків на базі ШІ та Інтернету речей, а доступність і можливість контролю даних у режимі реального часу допомагає максимально швидко запобігти будь-якій кібератаці[66].

---

[64]Звіт за 2020 про діяльність ГО “Міжнародний університет кібербезпеки”. URL:https://www.icu-ng.org/icu-ng/reports/annual-report-2020/

[65]The Impack of Artificial Intelligence on Cyber Secuirity. URL: https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/

[66] Кривенко П. Штучний інтелект на сторожі безпеки даних: інноваційні технології та хмарні сервіси допомагають забезпечити кібербезпеку. URL:https://cacds.org.ua/%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9-%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82-%D0%BD%D0%B0-%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%B6%D1%96-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D0%B4/

Використовуючи ШІ у боротьбі з кіберзагрозами, з'являється можливість більш ефективно реагувати або запобігати критичним загрозам, оскільки ця технологія дозволяє аналізувати величезні обсяги даних про ризики, тим самим скорочуючи час реагування та збільшуючи можливість раніше недостатньої безпеки.

Для того щоб вирішувати найскладніші проблеми у сфері кіберзлочинності і протистояти сучасним кібератакам необхідно випробовувати нові технології, намагаючись знайти кращі способи захисту, попередження або запобігання нападу. Звичайних методів захисту веб-світу недостатньо для реагування на загрози кібератак. Складність та частота таких випадків зростає з кожним днем. Технологічні досягнення сучасності, що забезпечуються ШІ та МН, дають кібербезпеці перевагу у забезпеченні багатьох онлайн-загроз. Кібербезпека є важливою для багатьох інших продуктів, що працюють на основі ШІ. Потрібно оцінювати внутрішню політику та вдосконалювати методології протидії таким кримінальним правопорушенням. В іншому випадку, без вдосконалення та розвитку не можливо підтримувати рівень безпеки, необхідного для захисту того, що є найважливішим[67].

[67]The Impact of Artificial Intelligence on Cyber Security. URL:https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/