МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Сумська філія
Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни **«Інформаційні технології в професійній діяльності»**
обов'язкових компонент освітньої програми другого (магістерського) рівня вищої освіти

262 Правоохоронна діяльність (правоохоронна діяльність)

за темою – «Нові тенденції злочинності епохи третьої і четвертої промислових революцій. Використання новітніх технологій у попередженні злочинів в розвинених країнах світу»

Суми 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 р № 7

СХВАЛЕНО
Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 29.08.2023 р № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 р № 7

Розглянуто на засіданні кафедри соціально-економічних дисциплін Протокол від 29.08.2023 р № 2

Розробники:
1. Професор кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх, кандидат технічних наук, доцент Струков Володимир Михайлович
2. Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС, к.е.н., доцент Виганяйло Світлана Миколаївна

Рецензенти:
1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, к.п.н., доцент Тетяна Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, к.е.н., доцент Олександр Борисович В'юненко

План лекції

1. Основні напрямки використання штучного інтелекту кримінальними співтовариствами.
2. Напрями використання роботів кримінальними і терористичними структурами.
3. Тенденції роботизації злочинності і тероризму.
4. Стратегічний підхід у використанні новітніх технологій цифрового світу в попередженні злочинів.
5. Використання для запобігання терористичним актам технологій, що дозволяють бачити крізь стіни.
6. Глобальна навігаційна система і електронне стеження з метою запобігання злочинам та актам тероризму.
7. Використання дронів проти браконьєрів, терористів і контрабандистів.
8. Застосування роботів в профілактичній і оперативній роботі поліції.
9. Нові технології прогнозування злочинної поведінки.

Рекомендована література:

1. Дрінь Б.М. Конспект лекцій з дисципліни “Сучасні інформаційні техногогії” для студентів спеціальності “Політологія”. Івано-Франківськ, ДВЗН “Прикарпатський національний університет”. 2016. 211 с. http://194.44.152.155/elib/local/3118.pdf

2. Клімушин П. С., Орлов О. В., Серенок А. О. Інформаційні системи та інформаційні технології в економіці. Навч. посіб. Харків. Вид-во ХарРІ НАДУ “Магістр”, 2011. 448 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/4730

3. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія.2018. 150 с .https://pidruchniki.com/15931106/politologiya/pravove_regulyuvannya_informatsiynoyi_sferi_ukrayini

4. Косиченко О.О., Махницький О.В. Захист службової інформації під час використання електронної Web-пошти на основі асиметричного шифрування з відкритим ключем за допомогою програми Mailvelope. Методичні рекомендації. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018.36 с. http://er.dduvs.in.ua/handle/123456789/233?subject_page=1

5. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності: навч. посіб. Дніпро: ДДУВС, 2018. 218 с. http://er.dduvs.in.ua/handle/123456789/2046

6. Методичні рекомендації проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції/ О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. 37 с. https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/eib2.pdf

7. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659

Текст лекції

1. Основні напрямки використання штучного інтелекту кримінальними співтовариствами.

Успішні злочинці, які працюють по крупному в таких сферах, як фінанси, великомасштабна контрабанда, нелегальна купівля-продаж інтелектуальної власності і т. п., - люди абсолютно раціональні. На даному рівні розробок в області штучного інтелекту у них немає необхідності привертати увагу, вербуючи в свої ряди команди найбільш просунутих стартапів, за якими полюють військові і розвідувальні спільноти, найбільші корпорації.

Понад 70% впроваджень в області штучного інтелекту припадає на США і приблизно 15% на Китай. Відповідно, основні приклади використання штучного інтелекту криміналом можна почерпнути з доповідей та інших джерел, що публікуються правоохоронними структурами США (китайські джерела більш засекречені).

На початку 2017 р ФБР провело велику конференцію, присвячену питанням використання штучного інтелекту правоохоронними органами та криміналом. На конференції було відзначено: дані Інтерполу, Європолу, ФБР і правоохоронних органів інших країн, результати досліджень провідних університетів дозволяють говорити, що в даний час відсутні ознаки цілеспрямованих зусиль криміналу зі створення власних розробок в області штучного інтелекту.

Ця обставина трактується багатьма практиками наступним чином: в найближчій перспективі ФБР і поліція, взявши на озброєння штучний інтелект, отримають вирішальну перевагу над кіберзлочинністю і іншими видами організованого криміналу.

Перш за все, прагнучи мінімізувати витрати і залучити до розвитку власного продукту максимальну кількість зовнішніх, в значній мірі безкоштовних, розробників, більшість провідних виробників платформ штучного інтелекту вже випустили платформи з відкритим кодом.

У кіберкримінала є з чого вибрати для створення власних потужних платформ штучного інтелекту. Практично всі розробки штучного інтелекту з відкритим вихідним кодом є контейнери. Контейнер - це платформа, на якій за допомогою API можуть монтуватися будь-які сторонні програми, сервіси, бази даних і т. п. Якщо раніше кожен при створенні власної програми або сервісу повинен був від початку до кінця спочатку розробити алгоритми, а потім, користуючись тією чи іншою мовою програмування, перевести їх в код, то сьогодні можливо створювати товари і послуги так само, як будівельники будують будинок - зі стандартних, доставлених на буд майданчик деталей.

Починаючи з 2016 р стрімко зростає сфера AIAS - штучний інтелект як сервіс. Компанії, які розробляють окремі елементи штучного інтелекту, і в першу чергу сховища даних, алгоритми глибокого навчання, алгоритми нейронних мереж, включаючи глибокі, а також програми обробки природної

мови та багатовимірних розрахунків, більш ніж в двох третинах випадків передбачають можливість використання їх розробок через API. Більш того, деякі компанії сьогодні дозволяють за відносно невелику плату брати напрокат своє програмне забезпечення в області штучного інтелекту. Якщо в разі API при необхідності правоохоронці можуть встановити характер використання програми, то при оренді таке неможливо.

Нарешті, ще п'ять-сім років тому в світі було 17 університетів, в яких студенти отримували першокласну підготовку в галузі досліджень і практичних розробок, пов'язаних зі штучним інтелектом. В ті часи правоохоронці цілком могли тримати на обліку кожну людину, що спеціалізувалася в професії з підвищеним рівнем небезпеки для середовища, і могли відслідковувати його кар'єру протягом усього життя. Сьогодні такої можливості більше немає. У Сполучених Штатах число університетів, які навчають комп'ютерним наукам на високому рівні, збільшилася до 40, і подібного роду навчальні заклади з'явилися по всьому світу. Утворилася ціла галузь онлайн навчання. Сьогодні для людей, що володіють необхідною початковою підготовкою, кращі університети відкрили безкоштовні онлайн курси за всіма компонентами штучного інтелекту. Викладені факти побічно вказують на активну підготовку криміналу до оволодіння штучним інтелектом. При цьому кримінал не збирається винаходити велосипед. Він стурбований тим, як навчитися на ньому їздити і виробити
найбільш ефективні маршрути.

На думку Інтерполу і ФБР, використання штучного інтелекту криміналом в Америці та інших розвинених країнах протягом найближчих п'яти років буде мати місце в декількох пріоритетних сферах. Їх об'єднує найбільш сприятливе для криміналу співвідношення трьох змінних: отриманий злочинний дохід, сукупні наведені витрати на підготовку, вчинення і приховування злочину і рівень ризику.

Основні напрямки використання штучного інтелекту кримінальними співтовариствами наступні.

Використання штучного інтелекту для компрометації та імплантації шкідливого «софта» в платіжні системи, в основному використовують протокол блокчейн і мають P2P архітектуру.

Однорангові платіжні системи витісняють процесингові компанії, і перш за все за рахунок економії витрат для клієнтів.

При цьому станом на 2016 р з майже 30 платіжних сервісів, побудованих на блокчейні, що діють в США, лише сім задовольняли вимогам комп'ютерної безпеки. Відповідно, під'єднання до платіжних сервісів і додавання до кожної транзакції приблизно 0,1-0,3% принесе мільярдні доходи злочинцям при відсутності будь-якого ризику.

1) На частку високотехнологічного кіберкримінала, що витягає **прибуток з торгових операцій найбільших фінансових інститутів**, доводиться 40-50 млрд дол. США щорічно. Це найбільш прибуткова, хоча і досить ризикована сфера організованої кіберзлочинності.

Оскільки протягом останніх кількох років розгорнулася справжня гонка фінансових озброєнь, що виражається в удосконаленні усіма найбільшими фінансовими інститутами своїх платформ на основі штучного інтелекту, злочинцям навіть для того, щоб хоча б зберегти частку доходів, необхідно брати участь в цій гонці. У зв'язку з цим використання ОЗУ штучного інтелекту для операцій на фінансових ринках шляхом проникнення і компрометації торгових платформ не залишає для криміналу іншої можливості, крім як використовувати кращі рішення з відкритим кодом в поєднанні з AIAS. На відміну від ситуації в платіжному бізнесі, де в 2017-2020 рр. очікується різке збільшення розмірів і частки злочинних доходів в обороті платіжних систем, в ***алгоритмічному трейдингу*** в короткостроковій перспективі частка злочинців буде знижуватися.

Є підстави вважати, що в міру розгортання технологічної гонки інтерес кіберзлочинців як всередині, так і поза США до інтелектуальної власності буде тільки наростати. Відомо також, що для розкриття сьогоднішніх могутніших систем корпоративно-інформаційної безпеки все ширше використовуються багатофункціональні програми, в основі яких лежать алгоритмічні модулі, що самовдосконалюються. Подібні модулі - це ключовий елемент штучного інтелекту.

Самі керівники ФБР вважають, що Америка сьогодні не готова до відсічі хакерським угрупованням, націленим на інтелектуальну власність, щоналежить корпораціям, федеральному уряду і університетам.

2) В умовах технологічної гонки впровадження нових продуктів, послуг і програм є імперативом виживання. Зрозуміло, що набагато вигідніше купити вкрадену документацію, креслення, програми, ніж витрачати величезні гроші на дослідження і розробки. Спільне дослідження Академії ФБР і фармацевтичного гіганта Sanofi показало на прикладі Індії, що 1 дол. вкраденої інтелектуальної власності в фармацевтиці економить виробникам дженериків 17-20 дол.витрат на дослідження і розробки.

Очевидно, що настільки прибуткова галузь є одним з ключових кандидатів на використання штучного інтелекту. Є дані, що вже в даний час всередині корпоративних мереж лідерів американського хайтека і біотехнологій діють багатоцільові і багатофункціональні хакерські програмні модулі, побудовані на основі самовдосконалюючихся програм.

Зазначені напрями використання штучного інтелекту злочинцями очевидні. Вони випливають з застосування до реальності тих критеріїв вибору сфери діяльності, якими керується організована злочинність в усьому світі.

Правоохоронці по всьому світу всерйоз готуються до появи підпільних синдикатів, що спеціалізуються на замовних високотехнологічних вбивствах, замаскованих під технічні інциденти різного роду. Беручи до уваги обсяг ринку замовних вбивств в Сполучених Штатах, що становить близько 2 млрд. дол. на рік, ми очікуємо появу такого мережевого синдикату, а швидше за все не одного, а декількох, в часовому інтервалі один-два роки.

Головним інструментом подібних синдикатів можуть стати не хакерські

програми самі по собі, а штучний інтелект. Тонкість тут в наступному. Різного роду автоматизовані автономні системи в переважній більшості керуються з єдиного обчислювального центру, який функціонує як штучний інтелект. Це називається ройовим навчанням. Відповідно, підключитися і замістити команди одного штучного інтелекту може тільки інший. Програмісту це не під силу. Він буде розпізнаний через більшу повільність і меншу алгорітмічність дій і операцій.

Крім того, тільки штучному інтелекту під силу замаскувати зловмисне відключення або виконання несанкціонованих дій технічною відмовою. Незважаючи на деяку екстравагантність, найближчим часом даний злочинний промисел може стати реальністю. Погано те, що особливо на першому етапі переважна частина подібних вбивств залишатиметься нерозкритими. У відділах по боротьбі з вбивствами просто немає фахівців, здатних на рівні професіонала розбиратися в тонкощах нейронних мереж, глибокого навчання і активного тестування.

Злочинці не гірше університетських професорів аналізують події і процеси і встановлюють причинно-наслідкові зв'язки.

Злочинні організації розуміють, що їм не під силу зруйнувати і скомпрометувати інформаційні бази правоохоронців.

Якщо злочинні співтовариства не можуть знищити бази правоохоронців, то вони, очевидно, підуть іншим шляхом. У будь-якій системі найвразливіший фактор - це людина. У всьому світі правоохоронці фіксують спроби на «чорному» ринку купити ті чи інші бази зображень з відеокамер, встановлених в кафе, торговельних центрах, поряд з поліцейськими дільницями, будівлями ФБР і т. п. Це наводить на думку, що злочинці почали створення власної бази даних з використанням приблизно тих же рішень штучного інтелекту, щоі правоохоронні органи. З урахуванням того, що обсяг їх бази буде істотно менше, її цілком можна реалізувати на платформах штучного інтелекту з відкритим кодом, з'єднавши їх з комерційно доступними сервісами аналізу зв'язків, відео, текстів і т. п.

Злочинці будуть намагатися створити свої бази шляхом аналізу потокового відео з місць, наближених до будівель правоохоронних органів. Перш за все цебаза агентів під прикриттям і інформаторів.

Можна очікувати також спроб створення криміналом баз даннях на співробітників інформаційних центрів поліції, тобто людей, допущених в «святая святих».

2. Напрями використання роботів кримінальними і терористичними структурами.

Ідея використовувати робота як знаряддя вбивства - абсолютно тривіальна. Першою людиною, загиблою від робота, став американський робітник С. Форд в 1970 і рр. Він працював на автоматизованому підприємстві, яке виконувало фарбувальні роботи для автомобільної індустрії. В результаті порушення програми, що відповідає за координацію

автоматичних маніпуляторів одного з роботів, останній замість дверцят схопив за шию робочого і задушив його.

З 2016 року відбулося перше цілеспрямоване вбивство з використанням робота. У палаті інтенсивної терапії госпіталю ордена єзуїтів в Сан Мігелі хворий помер від подачі в крапельницю смертоносного складу замість запропонованих ліків. Поліцейські не змогли б виявити цей злочин, якби не випадковість.

Програміст, якого банда підрядила, щоб зламати програму, що управляє автоматичної роздачею ліків, поділився інформацією в одному із закритих чатів. У ньому був присутній інформатор міської поліції. Завдяки йому програміст був затриманий, а пізніше прояснилася вся картина.

На відкритих конференціях ФБР зазначалося, що протягом 2015-2016 рр. агенти під прикриттям і інформатори неодноразово повідомляли, що злочинні синдикати прагматично серйозно обговорювали різні варіанти вбивств, використовуючи насичені електронікою автомобілі, «розумні будинки», медичні комплекси і т. п. Оскільки у злочинців зазвичай думки не розходяться зі словом, а слово - зі справою , цілком можна очікувати появи в Америці принципово нового явища.

У доповіді «Загрози і ризики використання автономних автоматизованих систем і роботів злочинністю, екстремістами і терористами», підготовленому в 2015 р. міждисциплінарним колективом дослідників з різних університетів США на базі МТІ на замовлення федеральних органів влади США, визначені можливості, ступені ризику і різноманітність загроз використання робототехніки злочинцями, екстремістами і терористами.

Можна виділити наступні основні напрямки використання ААС і робототехніки деструктивними організаціями.

Розвідка.

До останнього часу використання радіотехнічної, електронної, повітряної, підводної і іншої технологічно складної розвідки було прерогативою виключно державних структур, включаючи розвідувальні служби, правоохоронні органи і т. п. В даний час стан ситуація докорінно змінилася. Вперше в історії деструктивні організовані структури отримали можливість ведення розвідки по своїй технічній складності, а відповідно, і обсягом та якістю одержуваної і оброблюваної інформації, яка не поступається державним структурам. У вирішальній мірі це пов'язано не тільки з поширенням і розвитком Інтернету, але і з якісним стрибком в ААС і робототехніці. Якщо ще кілька років тому БПЛА, оснащений універсальним розвідувальним комплексом, що включає системи відеорозвідки, спостереження в інфрачервоному діапазоні, засоби перехоплення телекомунікаційних сигналів, коштував 300-350 тис. дол. США і виготовлявся виключно компаніями - підрядчиками Пентагону, то вже сьогодні, а тим більше завтра ситуація інша. В даний час такий комплекс може бути придбаний на легальному і нелегальному ринках будь-яким платоспроможним клієнтом, включаючи злочинні і екстремістські

структури, менш ніж за 50 тис. Дол. США. При цьому виробниками таких дронів-розвідників-спостерігачів вже сьогодні є понад 700 легальних компаній по всьому світу, включаючи країни Азії, Африки і невідоме число нелегальних виробників.

Також сьогодні доступні для деструктивних структур пересувні наземні розвідувальні комплекси, монтовані на автомобілі і що маскуються під позашляховики, мінівени, фургони і т. п. Дані комплекси, які (без вартості автомобіля) можна придбати в різних країнах світу легально і на «чорному» глобальному ринку коштують від 15 до 30 тис. дол. США. Вони дозволяють не тільки прослуховувати інформацію із закритих приміщень, використовуючи акустичні ефекти, але і знімати інформацію з розташованих в зоні дії комплексу комп'ютерів, планшетів і т. п.

У 2014 р. у Великобританії однією зі злочинних груп був замовлений і використаний розвідувальний комплекс, який, будучи поставлений недалеко від банку-сховища, дозволяв отримувати коди електронних банківських сейфів, знімаючи інформацію при їх відкритті законослухняними клієнтами.

Можна зробити прогноз, що протягом найближчих трьох - п'яти років основна частина розвідувальних комплексів, що знаходяться в руках деструктивних організацій, буде відноситися до засобів повітряного і наземного базування, відповідно, до дронів і розвідувальних автомобілів. У більш віддаленій перспективі слід очікувати освоєння деструктивними структурами морських глибин і космічного простору.

Транспорт.

Було б дивно, якби злочинні групи не скористалися сегментом військової і цивільної робототехніки, що найбільш швидко розвивається, а саме роботизованими транспортними засобами, не кажучи вже про військове використання автоматизованого транспорту для експедиційних, евакуаційних і логістичних потреб. За оцінками фахівців і бізнес-аналітиків, в автомобільній промисловості до 2020 р. не менше 25% вироблених в розвинених країнах автомобілів матимуть опцію автоводія. Відомо, що будь-яка висока технологія має потрійне застосування - військове, цивільне і кримінальне, тому є всі підстави вважати, що найбільш активно будуть застосовувати транспортних роботів терористи і злочинні синдикати.

Стосовно до терористів ця теза не потребує додаткової аргументації.

Терористичні структури, в тому числі мережевого і ройового типу, вже сьогодні мають ресурсні технологічні можливості, що перевершують потенціал багатьох державних армій. У зв'язку з цим терористи швидко і ефективно використовують всі види озброєнь і техніки, які застосовуються в сучасних арміях.

Що стосується злочинних транснаціональних організацій, то використання транспортної робототехніки дозволяє їм вирішити дві важливі задачі. З одного боку, воно дає можливість урізноманітнити канали доставки тих чи інших вантажів і звести до мінімуму людський фактор в цьому процесі. Останнє вкрай важливо. Наприклад, за даними американських правоохоронних структур, не менше 70% випадків розкриття злочинів і зриву

поставок наркотиків в Сполучені Штати пов'язано з успішною агентурною роботою або діяльністю агентів під прикриттям. Іншими словами, чим більше роботів і менше людей бере участь в злочинних акціях, тим складніше силам правопорядку впровадити в злочинні організації своїх людей або завербувати там агентів.

З іншого боку, використання транспортної робототехніки дозволяє будувати принципово нові логістичні системи.

Дрони.

За даними урядових та неурядових джерел в період 2000-2010 рр. всього 8% наркотрафіку з Мексики та інших латиноамериканських країн припадало на повітряні перевезення. У 2011-2014 рр. ця частка зросла більш ніж в два рази. За оцінками фахівців, до 2020 р. не менше третини наркотиків буде доставлятися повітрям, перш за все з використанням мікродронов, що летять на невеликій висоті до 100-150 м, або, навпаки, надвисоких дронів більшої місткості. В обох випадках виявлення таких дронів буде вкрай скрутним, особливо в умовах масового використання дронів в Сполучених Штатах як приватними особами, так і корпораціями. Якщо до недавнього часу більше 80% зафіксованих дронів, які перетнули американо- мексиканський кордон, що не були ідентифіковані як дрони, що належать легальним організаціям і приватним особам, то в найближчому майбутньому ситуація докорінно зміниться. В повітрі баражуватимуть безліч дронів, що належать законослухняним суб'єктам.

Колишній аналітик ФБР, а нині співробітник Google М. Гудман в книзі «Майбутнє злочинності» відзначав, що ще в 2011 р. в Лас-Вегасі був представлений невеликий дистанційно керований літак, який мав 11 антен і оснащений усіма можливими датчиками і камерами. Він отримав назву «WASP» і був спеціально розроблений для того, щоб перехоплювати сигнал Wi Fi всіх, включаючи зашифровані мережі. Він був також оснащений невеликим бортовим сервером Linux, який запускав різні хакерські пристрої, включаючи словник в 340 млн слів, що використовується для злому паролів. Камери пристрою дозволяли вести панорамну зйомку, а також зйомку в інфрачервоному випромінюванні, тобто знімати темну кімнату за склом.

Крім того, пристрій дозволяв записувати всі телефонні дзвінки в радіусі кілометра. Цей шпигунський безпілотник можна було придбати прямо на хакерському фестивалі всього за 6 тис. дол. США.

Гудман також пише, що кримінальні корпорації вже активно використовують дрони для транспортування наркотиків в Латинській Америці. Наприклад, в одній з в'язниць Сан Пауло дрони використовувалися для доставки півкілограма кокаїну для ув'язнених з волі, при цьому щодня. Подібні випадки зареєстровані в Канаді та Австралії.

У 2014 р. в Мексиці в одному з віддалених районів столиці країни поряд з авіаційним заводом компанії «Бомбардьє» завдяки агентурній розвідці був розкритий завод по збірці дронів різних конструкцій, що належить одному з наркосиндикатів. В ході розслідування з'ясувалося, що наркосиндикат підкупив керівництво заводу «Бомбардьє» і воно, нарікаючи

на низьку кваліфікацію мексиканських робітників, списувало в брак до 15% продукції. З деталей
«Бомбардьє» збирали в основному транспортні та наглядові дрони. При цьому в ході обшуку Агентству по боротьбі з наркотиками США (DEA) на заводі вдалося захопити конструкторську документацію, що свідчить про те, що наркосиндикат готувався налаштувати виробництво бойових дронів прикриття. Ці дрони повинні були супроводжувати транспортні дрони і виводити з ладу поліцейські автомобілі, оснащені радарами повітряного спостереження.

Починаючи з 2012 р. DEA задокументовано сотні випадків використання наркосиндикатами дронів для перекидання наркотиків, причому тільки в 7% випадків вдалося присікти доставку вантажів. Кримінальні умільці використовують дрони так само, як платформи для розміщення вогнепальної зброї. YouTube рясніє не тільки аматорськими зйомками дії саморобних бойових дронів, а й навчальними фільмами по створенню такого роду бойових дронів. У мережі Tor відкритий навіть відеоканал «Високі злочинні технології», де для скачування розміщуються навчальні фільми зі створення бойових дронів,роботів і т. п.

Найстрашніший сценарій, пов'язаний з розміщенням на безпілотниках біологічної, хімічної або радіологічної зброї. Наприклад, за 120 дол. США можна сьогодні купити дрон з радіусом дії 10 км зі змонтованим
розприскувачем сільськогосподарських добрив. Комплект передбачає, що режим розбризкування включається через пульт дистанційного керування при досягненні певного пункту GPS навігації. Якщо замість добрива завантажити якийсь смертоносний вірус, то ... (навіть думати не хочеться про те, що може статися).

Дрони можуть бути цілеспрямовано використані не тільки проти мас, а й проти конкретних осіб. В кінці 2013 р. канцлер Німеччини А. Меркель під час мітингу в Дрездені була приголомшена дроном, який сів до її ніг на сцені. Атака була проведена Партією піратів, яка заявила, що здійснила цю акцію, щоб переконатися, що канцлер розуміє, що говорить, коли вимовляє слова: « У Німеччині повинні бути законодавчо дозволені дрони для спостереження за громадянами». Хоча ніхто не постраждав, всі світові агентства розтиражували цю новину. А на YouTube вона перетворилася у вірусне відео.

У жовтні 2016 р. портал Life.ru повідомив, що російським спецслужбам стало відомо, що в штабі ІГІЛ створено підрозділ високотехнологічних терактів. Бойовики роблять ставку на малі керовані літальні системи: дрони з саморобними бомбами планується використовувати для терактів в країнах Європи. Експерти бачать в цій тактиці серйозну небезпеку: незважаючи на недосконаліть дронів і інших бойових роботів, цей напрямок тероризму буде тільки розвиватися.

У підрозділі є керівник, помічник, директор з навчання бойовиків одинаків, директор з планування терактів, фінансовий директор та інші фахівці, як розповіло джерело в спецслужбах. Саме цей підрозділ готує

теракти з використанням малих керованих літальних систем - дронів. Так бойовики збираються убезпечити самих терористів і учасників терористичного підпілля від загибелі. Перед командою, яка відповідає за розробку високотехнологічних терактів, стоїть завдання: акцій проводити більше, але самих терористів залучати до них менше. Найкраще, якщо це будуть поодинокі оператори. Це пов'язано з тим, що в останні роки абсолютна більшість планованих терактів за участю смертників було зірвано заздалегідь, тому і робиться ставка на одинаків.

Схема роботи буде приблизною такою: за вказівкою ватажка оператор-одинак снаряджає дрон саморобною бомбою, привозить його до місця акції, запусає і буде керувати ним дистанційно, як пояснило джерело в спецслужбах. Є інформація, що бойовики ІГІЛ планують обкатати високотехнологічні теракти в країнах Європи. Дрони будуть заряджені саморобними бомбами чи отруйними речовинами і управлятися дистанційно. Коли апарат з’явиться в людному місці або на об'єкті, бомба буде приведена в дію. Дрони в руках терористів можуть становити небезпеку як для місць масового скупчення людей, так і для різних об'єктів, що охороняються. Навіть якщо дрон помітять і зіб'ють, то при падінні він все одно встигне наробити лиха. У ньому може бути налаштована система автоматичного підриву бомби.

Крім того, поява і швидкий прогрес транспортних дронів різко розширить географію злочинності, особливо в частині наркотрафіку, контрабанди і, можливо, ринку торгівлі людськими органами. В даний час в умовах вкрай скрутної логістики з багатьох районів традиційного вирощування наркокультур типу Бірми, районів Афганістану, залучених у військові дії, регіонів Центральної Азії, що належать пострадянському простору, і т.п. вкрай витратно доставляти наркотики. Злочинним синдикатам доводиться нести високі логістичні витрати, пов'язані зі складністю і ризиками доставки. Вже наявні в даний час транспортні роботизовані засоби повітряного, наземного і підводного базування дозволяють недорого доставити будь-який відносно компактний вантаж з будь-якої точки світу в будь-яку точку світу. Відомо, що в 2014 р. відновлені великомасштабні поставки високоякісних наркотиків з районів «Золотого трикутника». У логістиці використовуються БПЛА і крокуючі наземні транспортні засоби.

В даний час в якості транспортних засобів найбільш широко використовуються дрони. Все частіше злочинні групи замовляють крокуючі транспортні засоби. Відомо також про розробку недорогих, доступних для будь- якого комерційного користувача підводних безпілотних роботизованих транспортних пристроїв.

Роботи-командос.

Роботи-командос є гібридом розвідувальних і транспортних робототехнічних систем, оснащених засобами виконання й інших цільових функцій. Наприклад, такі роботи здатні підніматися по вертикальних поверхнях, безшумно проникати в закриті приміщення і т. п. До

теперішнього часу вважалося, що такими роботами володіють спеціальні підрозділи армій США, Великої Британії та Ізраїлю. Відомо також, що наближається до завершення виробництво аналогічних систем для збройних сил Росії, Китаю і Южної Кореї. Однак в кінці 2014 р. британським тележурналістом в ході боїв між курдськими формуваннями (пешмерга) і бойовиками ІГІЛ в околицях міста Кабані на сирійсько-турецькому кордоні вдалося зняти двох роботів командос, які використовуються ІГІЛ. Немає сумніву, що терористичні організації різної локації в найближчі роки отримають в своє розпорядження роботів командос. Також можна прогнозувати в міру зниження їх вартості використання подібних робототехнічних систем і злочинними групами. У найближчі роки це навряд чи станеться, оскільки такого типу системи цікаві перш за все не для транснаціональної, а для локальної, міський, вуличної злочинності. Вона може використовувати подібних роботів для проведення грабежів, нападів на квартири і т. п. В даний час кожен робот-коммандос коштує до півмільйона доларів. Зниження ціни в 10 разів, коли вони стануть вигідними для вуличної злочинності, відбудеться близько 2020 р. або пізніше.

Бойові роботи.

Не тільки в електронних і друкованих ЗМІ, а й в урядових документах їхназивають роботами вбивцями. Роботами-вбивцями є повітряні, наземні і водні та підводні системи, оснащені бойовими компонентом. До останнього часу, як правило, використання терміна «робот» для цих пристроїв носило в переважній більшості випадків некоректний характер. Аж до 2013 р. практично всі системи, оснащені бойовими компонентом, припускали участь людини в якості оператора. Саме персонал в збройних силах США приймає рішення про вибір мети і нанесенні летального або нелетального удару. З 2014 року, згідно з наявними даними, на озброєння «Цхакаія» (Армії оборони Ізраїлю) надійшли бойові роботи.

Нанороботи.

Л. Дель Монте, відомий вчений фізик, колишній керівник розробок мікроелектроніки в IBM, автор книги «Нанооружие: растущая угроза человечеству», прогнозує, що до кінця 2020 х рр. терористи зможуть отримати доступ до нанозброї і будуть здатні використовувати нанороботів для здійснення терористичних атак, наприклад для зараження систем водопостачання великих міст або отруєння людей ін'єкціями.

Нанодрони, на думку Дель Монте, також можуть стати інструментами біологічної війни.

Ще в 2010 р Пентагон висловлював побоювання, що нанотехнології призведуть до створення вибухонебезпечного штучного мікропилу, наноботи зможуть доставляти біологічну зброю, виступати самі в ролі зброї. Наноботи навіть будуть потрапляти при диханні в легені солдатів і виводити їх з ладу. Дель Монте в своїй книзі прогнозує, що автономні наноботи будуть в змозі збирати свої копії, тобто відтворювати самі себе. Управління

мільйонами наноботів може стати величезною проблемою, а збої в програмному забезпеченні можуть привести до непередбачуваних наслідків. Взагалі, що стосується використання бойових роботів деструктивними організаціями, то є підстави очікувати, що це вже сталося або станеться в інтервалі від двох до п'яти років.

Дана проблема має кілька аспектів. Бойовий робот являє собою комбінацію звичайного багатофункціонального робота з добавкою бойового і керуючого компонентів. Вони виробляються і продаються окремо як на легальних, так і особливо на нелегальних ринках. Немає ніяких перешкод для того, щоб терористичні, злочинні і екстремістські групи найняли конструкторів, програмістів, які придбали б потрібну універсальну роботизовану платформу і змонтували на ній ті чи інші бойові компоненти. Ймовірно, що в ближній перспективі подібні кустарні бойові роботи будуть поступатися за своїми характеристиками бойовим роботам, які перебувають в розпорядженні збройних сил і сил правопорядку держав. Однак в перспективі в інтервалі від трьох до семи років можна очікувати вирівнювання потенціалу, можливостей і доступності бойових роботів для державних сил і деструктивних акторів.Бойові роботи різноманітного базування розрізняються за типами оснащення озброєнням. Найбільш широкого поширення набули бойові дрони, тобто Безпілотники, озброєні ракетами для ураження, як правило, наземних цілей. У 2014 р. на озброєння прикордонної служби та берегової охорони США, а також поліції декількох штатів надійшли бойові дрони, оснащені нелетальною зброєю, включаючи біобезпечні клеї, мережі, сльозогінний газ, паралізуючі речовини і т. п. Оскільки так само, як у випадку з бойовими дронами, подібні системи можуть бути створені невеликими групами фахівців, свого роду нелегальними стартапами, то є підстави вважати, що вони або вже є, або найближчим часом виявляться в розпорядженні деструкторів.

На відміну від роботів-вбивць, найбільш затребуваних терористами і екстремістами, подібні роботи будуть взяті на озброєння в першу чергу злочинними групами. Вони дозволяють здійснювати різного роду акції без вбивств людей. У разі припинення або розкриття подібних акцій це, без сумніву, знизить терміни покарання для їх організаторів і учасників. Дана обставина в більшості випадків приймається до уваги організаторами злочинних акцій.

Справжнім кошмаром для розвідувальних і правоохоронних структур усіх країн світу є бойові роботи, оснащені біологічною і хімічною зброєю. Щоб створити бойового робота, який використовує біологічну зброю, досить використовувати вироблені в даний час дрони сільськогосподарського призначення, заповнивши відповідні їх ємності не добривами, а бактеріями, вірусами або хімічними сполуками. Вартість сільськогосподарського дрона з дальністю польоту до 150 км і ємністю завантаження до 50 л становить лише 6 тис. дол. США, а ємністю до 200 л - менше 9 тис. дол. Купівля такого дрона доступна не тільки терористичним угрупуванням, а й окремій групі фанатиків і екстремістів.

Що стосується виробництва біологічної та хімічної зброї, то сьогодні немає ніякої можливості своєчасно розпізнати та ідентифікувати подібні процеси, організовані на розподіленій основі в лабораторіях американських, західноєвропейських і східно-азіатських університетів. Це є найбільшою і найбільш недооціненою небезпекою при використанні робототехніки терористами і екстремістами. На відміну від терористів і екстремістів злочинці можуть використовувати подібні засоби для шантажу органів влади, урядів з метою отримання великих фінансових коштів.

Ще більш небезпечним в перспективі є створення бойових роботів, озброєних спеціальними технічними пристроями безконтактного зараження програмно апаратних блоків різного типу, встановлених на військових, цивільних, транспортних та інших об'єктах. У 2014 р. американські та німецькі програмісти і технологи повідомили про те, що їм вдалося створити системи зараження програмних систем, навіть не підключених до Інтернету та інших комп'ютерних мереж, через оптичне і акустичне середовища. Представляється, що в ближній перспективі (до п'яти років) в силу експериментального характеру подібних робіт і їх миттєвого засекречування навряд чи слід вважати такою, що заслуговує уваги ймовірність оснащення подібною фізико-програмною зброєю бойових дронів, які перебувають в розпорядженні деструктивних структур.

З 2013 р. почалося оснащення бойових роботів, які перебувають в розпорядженні злочинних і терористичних організацій, засобами придушення систем виявлення і контролю технічних пристроїв, а також біологічних об'єктів в прикордонних зонах, територіях особливої охорони і т. п. Такі системи були в 2013-2014 рр. неодноразово застосовані проти правоохоронних підрозділів США на американо-мексиканському кордоні, структур берегової охорони в районі Флориди і Мексиканської затоки, берегової охорони Італії і т.п.

3. **Тенденції роботизації злочинності і тероризму.**

Технологізація вуличної і неорганізованої злочинності.

Традиційно використання складних технічних пристроїв і пристосувань було прерогативою організованої злочинності. В останні роки ситуація докорінно змінилася. З появою «Інтернету речей», по суті, весь навколишній світ перетворився зі світу речей в світ ААС. Це в повній мірі відноситься не тільки до сьогоднішніх складних систем управління будинком, а й до телевізорів, холодильників, пилососів, автомобілів і т. п. У найближчі п'ять - сім років очікується поява масового ринку побутової робототехніки. З дорогих іграшок і статусних пристроїв для багатих побутові роботи стануть обов'язковою приналежністю будинку і квартири середньої американської сім'ї.

М. Гудман в книзі «Майбутнє злочинності» наводить приклад, що стався на Тайвані в середині 2014 р. Поліція намагалась заарештувати відомого наркоторговця, який оточив свій будинок мережею роботів-відеоспостерігачів, озброєних вражаючими електрошоковими пристроями та сльозогінним газом. Збентежена поліція зіткнулася з незвичайним опором, а

наркоторговець сховався через заздалегідь підготовлений підземний хід.

В останні п'ять - сім років по експоненті зростає число злочинів - від грабежів до вбивств - з використанням ААС. Значна частина подібних злочинів, зафіксованих в поліцейських звітах, залишається нерозкритою. Це пов'язано з тим, що подібні високотехнологічні злочини, що здійснюються окремими особами або невеликими кримінальними групами, в корені відрізняються від традиційних правопорушень. Правопорушення, з якими звикла мати справу поліція, повністю відбуваються в реальному світі. Відповідно, злочинець залишає докази, або, більш того, він фіксується в минулому свідками або в останні роки різного роду системами відеоспостереження. Злочинність з використанням ААС і роботів припускає, безумовно, фізичні дії. Але сигнал, який приводить в дію ті чи інші апаратні засоби, передається в електромагнітному середовищі і носить віртуальний характер. Сьогодні для того, щоб скоїти злочин, не треба бути присутнім на його місці. Можна перебувати не за десятки, а навіть за сотні і тисячі кілометрів. Правоохоронні органи не звикли працювати в таких умовах, і, відповідно, їх діяльність не дуже ефективна.

Не кажучи вже про злочинні синдикати, навіть окремі, як прийнято говорити, вуличні злочинці усвідомлюють нездатність поліції протистояти високотехнологічним злочинам.

Саме тому вони беруть на озброєння ААС і роботів як знаряддя злочину. Наприклад, російські кіберзлочинці стали застосовувати новий спосіб розкрадання даних банківських карт за допомогою зовнішніх інтерактивних голосових відповідей (IVR). Шахраї використовують спеціально запрограмованих роботів, які телефонують клієнтам фінансових організацій. Програма видає себе за співробітника банку і легко вивідує всю необхідну інформацію (облікові дані, PINкоди, CVVкоди і т. д.). Як правило, IVR використовуються для відповіді на вхідні дзвінки (вітання клієнтів, пропозиції передзвонити на внутрішній номер співробітника банку та ін.). Шахраї стали застосовувати дану технологію для вихідних дзвінків. Представившись співробітником фінансової організації, робот просить нічого не підозрюваючого абонента повідомити дані або для уточнення деяких моментів, або через збій системи.

З метою приховати свої сліди зловмисники запускають роботів в «хмарних» дата-центрах (центрах зберігання і обробки даних). Для того щоб уникнути підозр з боку жертв, час від часу програма перенаправляє їх дзвінки на живих людей. Дана схема дуже ефективна, оскільки більшість клієнтів банків не здогадуються про здатність роботів дзвонити.

Підвищення ймовірності великомасштабних терористичних актів.

Тривалий час великомасштабні терористичні акти вимагали довгої підготовки, залучення багатьох учасників, витрат значних і різноманітних ресурсів і, нарешті, фізичної присутності терористів в зоні актів залякування і насильства. Найбільш яскравими прикладами стали акт 11 вересня 2001 р., вибухи в метро в Лондоні і на вокзалі в Мадриді. Всі вони мали зазначені вище риси. Силам національної безпеки не вдалося запобігти ці акти, але

зазначені вище характеристики дозволили їм вийти на планувальників і виконавців варварських актів і покарати їх. Ці ж риси дозволили силам національної безпеки різних країн запобігти в останні 15 років кілька десятків великомасштабних терористичних актів, які за своїми наслідками могли не поступатися і навіть перевершити події, що трапилися.

Енергетичні мережі незалежно від того, в чиїй власності та юрисдикції вони знаходяться, керуються ААС, з'єднаними з Інтернетом, як і системи міських водопроводів, каналізації, теплопостачання. Найнебезпечніше полягає в тому, що за останні п'ять - сім років ефективними роботизованими системами оснащені всі АЕС, найбільші греблі і т. п.У зв'язку з цим навіть не тривогу, а жах у фахівців в США викликали звісткипро те, що за останні роки непізнані хакери неодноразово вторгалися в систему енергопостачання, комплекси автоматизованого управління і сховища даних гідроспоруд і навіть атомних станцій США. В результаті у невідомих осіб або організацій є федеральна інформація про уразливість і недоліки систем управління і забезпечення безпеки усіма греблями і гідротехнічними комплексами на території США, системами водопостачання багатьох великих і найбільших міст країни, регіональних енергосистем. У разі ж, якщо інформація про уразливість в критичних інфраструктурах і системах управління ними вже потрапила або потрапить в розпорядження терористичних організацій, екстремістських угруповань і з дещо меншим ризиком - злочинних синдикатів, можуть статися непередбачувані за своїми наслідками акти. Причому на сьогоднішній день у структур національної безпеки немає способів запобігти їх. Більш того, утруднена буде ідентифікація нападника.

Згідно зі звітом компанії Trend Micro (травень 2017 г.) в світі налічується понад 83 тис. доступних через Мережу промислових роботів, і в 5 тис. з них відсутні механізми аутентифікації користувачів. Дослідники виявили в роботах 65 вразливостей, які, в тому числі, дозволяють обійти механізмиаутентифікації, модифікувати ключові настройки і змінити режим роботипристрою.

Все вищевикладене стосується лише роботів, безпосередньо доступних через Інтернет. Однак, як підкреслюють дослідники, зловмисники також можуть отримати доступ до не під'єднаних до Мережі пристроїв, попередньо зламавши промислові маршрутизатори, які використовуються на високотехнологічних підприємствах.

Наслідки кібератак на промислових роботів можуть бути катастрофічними. Згідно зі звітом Trend Micro в результаті подібних атак в вироблених продуктах можуть бути дефекти. Зловмисники здатні втручатися у виробничий процес і вимагати від виробника викуп за його відновлення, псувати продукцію, заподіювати шкоду механізмам і їх операторам, а також викрадати інформацію, що зберігається в пам'яті роботів (вихідний код, параметри продукції та іншу інтелектуальну власність). На підтвердження своїх побоювань дослідники здійснили показову кібератаку на промислового робота в лабораторних умовах. Експерти продемонстрували, як за допомогою атаки можна непомітно

змінити рух пристрою. Програмний код залишається незмінним, а зміну руху неможливо вловити неозброєним поглядом. Проте найменше відхилення у виробничому процесі може привести до серйозних наслідків.

Нові виміри фінансового тероризму та організованої злочинності.

Якщо на споживчому ринку продаються перші дрібносерійні повноцінні роботи, а у військовій сфері на озброєння надходять перші поодинокі зразки, то в сфері фінансів повністю роботизовані системи - торгові роботи - за останні п'ять років стали звичайними на більшості фінансових ринків Америки,Великобританії та Японії. Торгові роботи представляють собою інтелектуальні програмно-аппаратні комплекси, які оснащені не тільки модулями збору, обробки, аналізу інформації, а й самостійного, без людини, прийняття рішеньзгідно алгоритмам. На останнє хотілося б звернути особливу увагу. Не тільки серед політиків, військових і бізнесменів, але навіть серед частини фахівців з інформаційних технологій існує помилка, що торгове роботи представляють собою предтечу штучного інтелекту і впритул наблизилися до нього. Зовні справа виглядає саме таким чином, оскільки всі рішення про куплю-продаж акцій, індексів, валют, деривативів і т. п. приймають безпосередньо програмно- аппаратні комплекси - торгові роботи. Але якщо звернутися до суті справи, то з'ясується, що рішення вони приймають не за власними правилами, які створили самі, а по алгоритмам, які закладені в них людьми - програмістами, розробниками, математиками, аналітиками і т. п. Тому про штучний інтелект говорити поки передчасно, хоча рішення на фінансових ринках приймаютьсяроботами без безпосередньої участі людини.

Якщо у 2010 році не більше третини операцій на американських фінансових ринках здійснювалося торговими роботами, то в даний час більше 70% угод на біржових і позабіржових фінансових ринках, які торгують біржовими фінансовими продуктами, здійснюються не людьми, а торговими роботами.

Експансія торгових роботів, які можуть коштувати 10 млн дол. і більше, пов'язана з двома обставинами. З одного боку, торгівля на фінансових ринках вимагає регулярної обробки величезних масивів інформації. При короткостроковому трейдингу, а на нього припадає основна частина операцій, люди просто не встигають опрацювати і проаналізувати різнорідні і різноформатні масиви інформації. Ефективніше це роблять торгові роботи, які приймають рішення на основі деяких правил. У цьому сенсі торгові роботи є спадкоємцями і більш універсальними варіантами комп'ютерів, які в минулому обігравали чемпіонів світу з шахів. В обох випадках в основі програм лежать певні алгоритмічні правила, побудовані на основі ієрархії прийняття рішень. З іншого боку, сьогодні відомо, що джерелом доходів на фінансових ринках є короткострочний часовий арбітраж. Якщо хтось встигає зреагувати на ринкові звістки швидше за інших, то він отримає вигоду від більш раннього знання тієї чи іншої новини. З середини минулого століття до нашого часу почалася гонка за швидкість реагування на інформацію.

Як було показано на прикладі бойових роботів, автоматизовані системи здатні швидше людей реагувати на будь-яку зовнішню інформацію. Відповідно, з середини 2010х рр. стали створюватися не тільки все більш досконалі алгоритмічно, але і все більш швидкодіючі торгові роботи. В даний час торговіроботи найбільших американських банків, які стоять вже не десятки, а сотні мільйонів доларів, окупаються трохи більше ніж за чотири місяці за рахуноктого, що здатні випереджати інших роботів на соті мілісекунди.

Панування торгових роботів на фінансових ринках створило нові загрози для фінансової системи і національної безпеки США і Заходу. У 2014 р. федеральна Комісія з цінних паперів (SEC) випустила доповідь, в якій звернула увагу не тільки фінансистів, а й політиків і структур, що займаються національною безпекою, на насторожуючий факт. Якщо протягом нульових років в середньому за рік фіксувалося трохи менше дев'яти непояснених коливань курсу акцій, в рази перевищують їх нормальну волатильність, то в 2011-2012 рр. подібних коливань фиксувалось вже в середньому 36 за рік, в 2013 р - 41 і в 2014 р - 74. Докладний аналіз, проведений SEC, показав, що ці коливання не були пов'язані з будь-якими подіями або новинними приводами, пов'язаними з відповідними компаніями. Ці коливання були результатами дій торгових роботів, які приймали рішення про купівлю-продаж відповідно до деяких алгоритмів. Після публікації доповіді ряд найбільших фінансових інститутів і незалежних трейдерів, чиї торгові роботи активно брали участь в операціях по закупівлі-продажу, що призвели до підозрілої сверх волатильності в 2013-2014 рр., із залученням фахівців Комісії, працівників Агентства національної безпеки (АНБ) і незалежних фірм з комп'ютерної безпеки здійснили програмно- технологічий аудит своїх роботів. В результаті з'ясувалося, що в більшості випадків (точна кількість з міркувань комерційної таємниці і національної безпеки озвучена не була) торгові роботи виробляли помилкові рішення в тому сенсі, що діяли не за алгоритмами, а в результаті зараження спеціальними шкідливими програмами, термін існування яких вимірювався секундами. Після оприлюднення даної інформації ФБР і незалежні експерти зробили висновок про те, що у всіх зазначених випадках мало місце не просто хакерство, а ретельно сплановані і віртуозно здійснені фінансові злочини з використанням програмно- апаратних комплексів.

Доступні дослідникам і громадськості факти говорять про те, що з кожним роком кількість і масштаби такого роду злочинності, пов'язаної із зараженням, а в майбутньому, можливо, і перехопленням управління торговими роботами, буде тільки наростати.

Поки достовірно відомо лише про факти фінансової злочинності з використанням торгових роботів. Однак з огляду на кластеризацію деструкції, є підстави вважати, що з кожним роком буде збільшуватися небезпека великомасштабних, а можливо, і глобальних актів фінансового тероризму. Імітаційні моделі, розроблені в Массачусетському технологічному інституті і Фінансової лабораторії в Швейцарії, в Цюріху,

свідчать, що вже сьогодні цілеспрямоване перехоплення управління торговими роботами може викликати глобальний крах фінансових ринків, за яким послідує відповідно до ефекту доміно колапс світової фінансової системи.

Кримінальний 3D друк.

3D друк подібно Інтернету принесе в життя і нові ризики. Природно, першим об'єктом злочинців в світі 3D друку стане крадіжка інтелектуальної власності. До теперішнього часу пірати крали музику, відео, ігри, програмне забезпечення. Тепер ситуація докорінно зміниться. Хоча вже кілька десятиліть шахраї спеціалізуються на підроблених сумках, одязі знаменитих фірм, виготовленні підроблених годинників Картьє і т. п., всі вони легко розпізнавалися внаслідок поганого дизайну і дешевих матеріалів. Однак в майбутньому досить буде відсканувати будь-яку, саму досконалу, модель, розпізнати, який матеріал використовується, і в точності відтворити його на 3D- принтері.

Цифрове виробництво також буде благом для зломщиків і злодіїв. Уже сьогодні, скориставшись фотографією з дому або офісу, де зображені ключі від них, випадково залишені на столі, можна продублювати ключ за допомогою 3D- друку. У 2012 р. поліцейські виявили програмне забезпечення для виготовлення ключів, що дозволяють злочинцям змінити цифрові браслети, що одягаються на них при домашніх арештах.

В майбутньому 3D-друк знайде велике застосування в наркоторгівлі. Вчені вже розробили так званий хімпьютер, який на вимогу друкує на 3D-принтері із заготовки ібупрофен. Мафіозні структури, безсумнівно, адаптують технологію 3D-друку для своїх потреб.

Можливо, одним з найгостріших питань є здатність 3D-друку виробляти вогнепальну зброю. К. Вілсон, 26-річний колишній студент, анархіст і лібертаріанець, шанувальник Страшного пірата Робертса, створив проект «Wiki зброя». Він поєднав його з біткойном, розмістив в «темному» інтернеті і організував розподілену онлайн-мережу з проектування, дизайну та друку на 3D- принтері різних зразків зброї.

Його найбільшим досягненням стали автоматична гвинтівка, яка змогла зробити 600 пострілів, і бойовий пістолет, що стріляє стандартними кулями. До теперішнього часу всю документацію, необхідну для друку пістолета на домашньому 3D-друк, завантажили 100 тис. осіб по всьому світу. Відповідаючи на питання в пресі, навіщо він це зробив, Вілсон сказав: «Комп'ютер, Інтернет і 3D-друк дали мені можливість реалізувати американську Конституцію, яка передбачає право громадян озброюватися».

Пластикова вогнепальна зброя особливо небезпечна, оскільки вона непомітна для стандартних детекторів безпеки, встановлених в урядових будівлях, аеропортах і т. п. Зайвий раз це довела команда ізраїльських відставних воєнних, які два рази поспіль пронесли в добре охороняєму і захищену поясами безпеки будівлю Кнесету надрукований на 3D-принтері пістолет. Аналітичний центр ФБР вкрай стурбований тенденцією виробництва 3D-зброї і недавно скупив всі існуючі моделі 3D-принтерів,

щоб дослідити, які з них терористи можуть використовувати для виготовлення саморобної вогнепальної зброї та вибухових пристроїв. Уже сьогодні складні промислові принтери, які тим не менше продаються всім платоспроможним клієнтам, дозволяють виготовити не тільки дрібну, але і велику зброю, включаючи основні деталі для пускових установок ракет «земля - земля» і «земля - повітря».

В умовах цифрового виробництва інспекція на державному кордоні стає безглуздою. Якщо можна просто надрукувати гармати, таблетки, бомби, то навіщо переходити кордони і ризикувати. 3D-друк ставить принципово нові питання перед міжнародною безпекою. Треба розуміти, що в умовах мініатюризації виробництва, багатофункціональних роботокомплексів і 3D-друку більше неможливо буде встановлювати ембарго на постачання зброї або чогось подібного в ті чи інші регіони.

Першопрохідцем у створенні зброї на 3D-принтерах став уже згаданий американець К. Вілсон, що представив в травні 2013 р свій винахід - однозарядний пістолет Liberator, креслення якого вільно стали «розгулювати» по Мережі. Дуже скоро це змусило владу США прийняти закон, який забороняв створювати подібні пристрої, а також ввести 10-річний мораторій на виготовлення зброї без додавання металу.

Це рішення виявилося своєчасним, але малоефективним. Роздрукований на 3D-принтері пістолет несе велику небезпеку для громадського спокою. Пластмасові деталі, з яких він роздрукований, ніколи не «запищать» на металодетекторі, а це значить, що пронести його на борт літака або увійти з ним в будівлю буде вельми просто. Також такий пістолет можна легко утилізувати - досить спалити знаряддя злочину, і ніяких слідів його існування не залишиться. А самозарядна гвинтівка Shuty, створена американська ентузіастом під ніком Derwood, поклала початок епосу автоматичної і напівавтоматичної зброї. Тепер такі пристрої здатні витримати від 10 до 30 пострілів і не розплавитися.

У 2014 р. 28-річного японця відправили до в'язниці за виготовлення пістолетів на 3D-принтері. Окружний суд Йокогами засудив Йосімото Імуру до ув'язнення за звинуваченням в незаконному володінні зброєю. Як пишуть місцеві ЗМІ, органи правопорядку зацікавилися молодою людиною після відеозапису. На ній він стріляв з виготовленої зброї в лісі і розповідав про його характеристики. Суд визнав, що практика друку пістолетів на 3D-принтері ставить під загрозу безпеку інших людей.

У 2015 р. 3D-друкована зброя (і деталі від неї) було знайдено у людей, пов'язаних з австралійськими кримінальними угрупованнями. А в 2016 р. поліція затримала байкера, у якого вдома були знайдені 3D-принтер і обладнання для виготовлення 3D-друкованої вогнепальної зброї.

На початку 2015 року під час поліцейської облави в Голд-Кості (Австралія) було знайдено кілька комплектів для збірки 3D-друкованих пістолетів. Трохи пізніше поліція виявила заряджений пістолет в Мудгеерабе, передмісті того ж міста. В останньому випадку теж було заарештовано кілька байкерів.

Після цього австралійське уряд зважився на круті заходи. З листопада 2015 р. у штаті Новий Південний Уельс було заборонено зберігати у себе навіть креслення 3D-друкованого зброї. Тепер за законом жителі цього штату можуть отримати до 14 років позбавлення волі за зберігання подібних цифрових креслень. На недавно проведеної прес-конференції поліція Нового Південного Уельсу продемонструвала два 3D-друкованих пістолета, зроблених за кресленнями «Визволителя» (Liberator), узятими з Мережі. На їх друк потрібно всього 27 годин, після чого досить встановити сталевий стержень, який виконує роль бойка ударника.

Біотехнології, тероризм і злочинність.

Можна багато говорити і писати про перспективи гуманістичного використання біо- та нанотехнологій, про «світле майбутнє» людства, про ліберальну євгеніку, про лікування спадкових захворювань, продовження людського життя нескінченно. Але все це стосується лише легальної частини біо- та нанотехнологічної революції. А існує, і вже тривалий час, нелегальна (і практично завжди кримінальна) її складова. Навіть коли цю нелегальну частину реалізує держава, нехай навіть сама суперліберальнодемократічна, вона завжди це робить потай від своїх громадян, своїх демократичних інститутів. І завжди така діяльність фактично противоправна і злочинна. Злочинна тому, що являє собою діяльність, заборонену міжнародно-правовими документами та національним кримінальним законодавством.

За оцінками експертів, лабораторія з виробництва біологічної зброї в сучасних умовах разом з усім обладнанням може коштувати в межах від декількох десятків до декількох сотень тисяч доларів США, а в якості біологічної зброї можуть бути використані і ті патогени, які конвенціонально заборонені для застосування в дослідницьких цілях, отримання діагностичних систем, вакцин та інших медичних препаратів.

Найбільш значущими загрозами біотероризму є різке збільшення числа фахівців з біотехнологій, доступність інформації за рецептурами біологічних та бактеріологічних препаратів, а також можливість легендування окремих актів біотероризму під прояви природних епідемій та інфекцій.

В кінці 2005 р. генетик Р. Брент з Каліфорнійського інституту молекулярних наук (Molecular Sciences Institute - MSI) провів експеримент, який доводить, що сьогодні технології в генній інженерії досягли вже такого рівня, коли один розумний лаборант з невеликим обсягом «правильних» ресурсів може виготовити біологічну зброю зі згубною міццю, яка не поступається атомній бомбі. Брент стверджує, що штучно сконструювати віспу, або сибірську виразку, або, може, навіть Ебола зараз можна в простій лабораторії, використовуючи вихідні компоненти, що вільно продаються і, таким чином, не викликаючи підозр. Наприклад, через Інтернет на мережевому аукціоні можна придбати будь- які моделі ДНК-синтезаторів: від 5 до 43 тис. дол. США. Щоб зібрати геном віспи, потрібно через Інтернет закупити сировини на 200 тис. дол. США. Генетичну послідовність можна

також легко знайти на публічних ресурсах Інтернету. Крім того, зараз існує чимало біотехнологічних фірм, які синтезують генетичні послідовності на замовлення і висилають клієнтові поштою.

Американський вчений Р. Карлсон, фізик і біолог, який працював деякий час з Брентом в MSI, прогнозує, що приблизно протягом десятиліття створення біологічної зброї з нуля стане настільки ж легким і дешевим, як побудова сайту. У червні 2006 року співробітники британської газети The Guardian з'ясували, що створити біологічну зброю сьогодні може буквально будь-який зацікавлений в цьому житель Сполученого Королівства. Напрямки тіньового (кримінального) використання результатів біотехнологічної революції і суб'єкти, що їх здійснюють[1]

Направления	Субъекты				
	Военные и спецслужбы	Мафиозные структуры	Террористы	Параученые (ученые-маньяки)	Фашисты и расисты
Разработка биологического, генетического («этнического» и т. д.) оружия	+	+	+	+	+
Создание «сверхчеловека» (сверхсвойств человека: повышенная агрессия, выносливость, нечувствительность к боли и т. д.)	+	+	+	+	+
Разработка нейрофармакологических средств для контроля поведения	+	+	+	+	+
Создание клонов человека	+	+	+	+	
Создание человекоподобных химер	+	+	+	+	
Торговля человеческими органами и тканями под видом продуктов генной инженерии		+			
Индустрия криминальных абортов (использование эмбрионов для экспериментов со стволовыми клетками)		+			
Использование генной инженерии для выведения устойчивых сортов наркотикосодержащих растений		+			
Использование достижений синтетической биологии по озданию трансгенных дрожжей в качестве сырья для опиатов		+			

Увагу журналістів привернув сайт компанії VN Bio Ltd, що займається постачанням обладнання та витратних матеріалів для біологічних

лабораторій. В одному з каталогів біосировини були знайдені досить дивні «товари» - на продаж виставили фрагменти ДНК смертельно небезпечних для людини вірусів віспи та іспанського грипу. Для оформлення замовлення на ДНК віспи знадобилося лише назвати адресу, номер мобільного телефону та адресу електронної пошти - вже через три години до редакції The Guardian подзвонив кур'єр і повідомив, що замовлення доставлено. Ніяких перевірок того, кому відправляється потенційно небезпечний вантаж, проведено не було - одержувачем міг би виявитися як законослухняний вчений, так і можливий терорист.

У цих умовах контроль за біотехнологічним ринком в Мережі повинен стати важливим новим завданням поліцейських підрозділів і спецслужб, контролюючих тіньові кримінальні ринки в Інтернеті.

Нейрофармакологічні засоби для контролю за поведінкою.

Не меншу небезпеку становить розробка нейрофармакологічних засобів для контролю за поведінкою. Про те, що і ці роботи проводилися, написано досить багато книг на вагомому фактичному матеріалі. По суті, мова тут йде про розроблені види психотропної зброї на основі біотехнологій. Ще в кінці 1950-х рр. А. Берл, в той час помічник державного секретаря США, який брав участь в програмах ЦРУ з контролю за поведінкою за допомогою нейрофармакології, в своєму щоденнику записав: «Я побоююся одного. Якщо вчені зроблять те, що запланували, то люди перетворяться в маніпульованим мурах».

Біотехнології в епоху біотероризму.

Фактично в XXI ст. почалася епоха біотероризму. Перший випадок був пов'язаний з розсилкою в 2001 р. поштою спор сибірської виразки, в результаті чого загинули п'ять осіб зі складу працівників Конгресу США, що мали контакт зі смертоносними конвертами. У 2014 р. спецслужбам США стало відомо, що імовірно в Ємені і на півночі Сирії «Аль-Каїда» створила лабораторії з виробництва біологічної зброї.

Ще в 1995 р японська терористична релігійна секта «Аум Сінрікьо», керівників якої брав і підтримував один з тодішніх російських лідерів, провела хімічну атаку в метро Токіо, в результаті якої загинули 300 осіб і близько 10 тис. серйозно отруїлися. В ході судового процесу стало відомо, що ця атака була лише репетицією передбачуваної масованої біоатаки проти Токіо з використанням надзвичайно небезпечного біотоксину, на розробку і виробництво якого секта витратила 10 млн дол. США.

Терористам більше не доведеться витрачати кошти і шукати фахівців, які могли б створити для них патогени і біологічну зброю. З появою синтетичної біології їм просто достатньо зламати ті чи інші сервери, скачати біопрограммную інформацію і самим роздрукувати смертоносні віруси. Звісно ж, що великих проблем в цій галузі у них не виникне. Адже, наприклад, генетичні коди вірусу еболи і знаменитої іспанки, яка забрала життя десятків мільйонів людей, можна скачати в Національному центрі біотехнологічної інформації в США.

Ще п'ять років тому синтетична біологія та генна інженерія були дорогим заняттям. Тепер вони по кишені невеликим і небагатим угрупованням, а в найближчі два роки стануть доступні кожному, хто витратить кілька тижнів на вивчення відповідної літератури і оволодіння практичними навичками роботи.

М. Гудман в книзі «Майбутнє злочинності» пише, що біопреступнікі і біотерористи не будуть покладатися на існуючі патогени, проти яких є засоби боротьби. Вони, безумовно, будуть створювати ще більш смертоносні нові віруси, проти яких немає антидотів. Що це неважко зробити, показали в 2013 р. дослідники з Нідерландів. При бюджеті в 100 тис. дол. США на основі штаму пташиного грипу вони змогли спроектувати і створити новий штам, який передається повітрям і швидко засвоюється людиною. В даний час пташиний грип для птахів і тварин має показник смертності 70%, але лише один з тисячі людей заражається пташиним грипом. Для нового штаму показники становили 98%, і з 100 інфікованих хвороба могла початися більш, ніж у 80%.

Таким чином, було створено по-справжньому страшна зброя, оскільки вірус передавався по повітрю. Дослідники провели роботу виключно для того, щоб привернути увагу наукової громадськості і політичних діячів до теми синтетичної біології і ввести заборону хоча б на проведення приватних досліджень в цій сфері, а також в будь-яких лабораторіях, які не підпадають під узгоджений в ООН список. Свою роботу з детальним викладом результатів проведених експериментів вчені розіслали в цілий ряд провідних наукових журналів. Але ні в одному стаття не вийшла. Втрутилися американський уряд і Наукова рада ЄС, які наклали вето на будь-які публікації в цій сфері. В результаті публікація розійшлася серед біологів у вигляді поштового файлу.

Біотерор, безсумнівно, може мати руйнівні наслідки. Але знову пошлемося на Гудмана. Він вважає, що з використанням досягнень синтетичної біології знову відродиться індивідуальний точковий терор. Технології синтетичної біології уможливлюють не тільки створення персоніфікованих ліків, але і персоніфікованих знарядь вбивства. Для цього треба лише синтезувати ДНК людини з конкретним вірусом або патогеном. У цьому випадку досить ввести соту частку міліграма цього патогена в їжу, розчинити в повітрі і т. п., і людина буде убита, а всі інші нічого не відчують.

Наркокартелі і синтетична біологія.

Вигідним напрямком діяльності мафіозних структур вже стало використання генної інженерії для виведення стійких сортів наркотиковмісних рослин (підвищення їх врожайності, захист від шкідників і т. д.) і створення нових видів наркотиків на основі технологій синтетичної біології.

Один з головних доходів організованої злочинності в XX і XXI ст. - виробництво і збут наркотиків. Як правило, наркокартелі отримують свій головний наркодоход не від роздрібної реалізації, а від вирощування або

синтезу наркотиків, їх очищення, упаковки, транспортування і оптових продажів по всьому світу. Це складний бізнес, який потребує високого рівня логістики, організації, управління і здатності реагувати на форс-мажорні обставини. Тому ще з 50 х рр. минулого століття наркокартелі фінансують науку, наймають до себе на роботу колишніх високопоставлених і професійних працівників спецслужб і правоохоронних органів, першокласних управлінців. Однак, цілком ймовірно, на багатьох ринках звичні(традиційні) наркокартелі доживаютьостанні дні.

На думку М. Гудмана, в найближчі 10 років традиційні наркокартелі будуть обмежені в своїх діях ринками країн, що розвиваються. Що стосується самих ємних ринків Америки, Європи, багатих країн Азії, то тут наркокартелі, що базуються на сільському господарстві, замінять високотехнологічні мережеві структури, що виробляють принципово нові види наркотиків, використовуючи технологи синтетичної біології. Це дозволить новим структурам різко підвищити в порівнянні з нині існуючими наркокартелями свою невразливість, заощадити значні ресурси на логістиці і організації системи продажів. Синтетична біологія буде використана злочинцями не тільки для створення наркосиндикату нового типу, але і для організації паралельної медицини.

Протягом останніх десятиліть ми бачимо неухильний перехід від рослинних наркотиків до синтетичних. Однак при всій своїй привабливості для наркоманів вони володіють таким числом побічних, нерідко смертельних ефектів, що навіть самі запеклі наркомани підсаджуються на них лише в кінці свого наркошляху.

Синтетична біологія дозволяє, якщо можна так висловитися, з'єднати споживчу ефективність штучних наркотиків з звичністю і відносної м'якістю рослинних. В рамках синтетичної біології більше не потрібно буде вирощувати рослини. Досить буде взяти генетичні коди марихуани, маку, листя коки і т. п. і синтезувати їх з дріжджами. Потім в принципі можна зробити наркотичний хліб, пиво або що завгодно. Це не тільки знизить витрати і відкриє нові ринки, а й зробить для правоохоронних органів вкрай складним розпізнавання систем збуту наркотиків.

У 2014 р М. Гудман в книзі «Майбутнє злочинності» наводив такі приклади. У лабораторії Північно-Західного університету США біоінженери створили синтетичну бактерію, в якій активний інгредієнт каннабіса був упакований в оболонку добре засвоюваній організмом бактерії для того, щоб доставляти знеболюючe безпосередньо в ході операції, причому в дозуванні, необхідному для тих людей, у яких є алергія на традиційні знеболюючі, що робить неможливим проведення їм складних хірургічних операцій.

Поєднання технологій синтетичної біології з технологіями 3D-друку призведе до того, що можна буде просто замовити картридж з певним набором хімічних елементів, вибрати в програмі потрібну речовину і друкувати - можна і аспірин, можна і амфетамін.

4.Стратегічний підхід у використанні новітніх технологій

цифрового світу в попередженні злочинів.

Британський бізнес, особливо ключова галузь господарства - фінансова, вимагає від поліції якісного підвищення рівня протидії високотехнологічній злочинності. Для цього планується продовжити роботу по формуванню спеціалізованих підрозділів по кіберзлочинності.

Разом з тим всі британські поліцейські повинні мати доступ до баз даних і сучасних інструментів, що забезпечує ефективні комунікації, профілактику і розслідування злочинів з використанням інформаційних технологій. Настав час, коли всі британські поліцейські, незалежно від віку, повинні пройти прискорені курси підготовки в галузі використання інформаційно-комунікаційних технологій.

Аналіз великих даних. Якщо раніше громадськість цікавили насамперед процедури доступу до персональних і корпоративних даних, то в найближчі роки необхідно, не чекаючи кризи громадської думки, чітко регламентувати доступ правоохоронних структур до потокових відеоданих, протоколів платіжних систем і протоколам «Інтернету речей». Уже сьогодні дані, в тому числі геолокація, одержувані зі смартфонів, дозволяють розкрити і запобігти багатьом серйозним злочинам. Потенціал даних з «Інтернету речей» набагато вище ефекту від даних геолокації зі смартфона.

Якщо поєднати три компоненти: створення потужних, доступних аж до низового рівня, баз і сховищ даних; укомплектованість поліції аналітиками даних і фахівцями з даними; підвищення рівня комп'ютерної грамотності поліцейських, аж до низового рівня, можна здійснити революцію даних. Ця революція дозволить:

- все ширше і з кращими результатами переходити від запобігання до профілактики злочинів;
- використовувати інформацію не тільки з поліцейських баз, а й з інших державних і приватних баз, які дозволяють випереджаючим чином виявляти осіб і групи, вразливі для злочинців;
- заздалегідь розпізнавати підозрілі моделі діяльності і сліди як тих, що готуються, так і вже скоєних злочинів. Найбільший ефект тут може дати поєднання аналітики електронних платежів з відеоаналітікою і аналітикою здійснюваних покупок;
- перевести дискусії щодо рівня криміналізації та уразливості різних сфер діяльності, видів торгівлі і сегментів ринку з загальнотеоретичного, експертного аналізу на мову документованої статистики. З'ясування тенденцій, куди кримінал спрямовує свої основні зусилля, дозволить поліції з випередженням реагувати на зміну обстановки;
- поряд з підвищенням рівня розкриття злочинів і все більшим перенесенням роботи з розслідування на профілактику і попередження кримінальних дій посилити контроль суспільства над поліцією. Контролюючі органи як всередині поліції, так і поза нею зможуть в автоматизованому режимі виявляти всі випадки необґрунтованої відмови в порушенні кримінальних справ, пов'язаних з використанням високих технологій.

У ситуації, коли в самій поліції немає фахівців необхідного рівня у

напрямку аналітики даних, вихід був знайдений в тісній співпраці з кращими британськими університетами. У взаємодії з університетським дослідницькими групами поліції цих міст зуміли вийти на досить високий рівень прогнозування ризику традиційних злочинів, наприклад таких, як крадіжка зі зломом, по окремих районах міст, аж до кварталів, а іноді і будинків. Після того, як на основі даних предикативного аналізу поліцейські міські структури змінили графіки і розподіл патрульних екіпажів, вдалося протягом 2015-2016 рр. домогтися зниження злочинності, еквівалентного зниженню традиційної злочинності, пов'язаної з крадіжками зі зломом сумарно за попередні сім років. Ці результати справили величезне враження як на поліцейські сили, так і на населення і бізнес. Поліцейські перестали боятися високих технологій, а бізнес став більш охоче жертвувати кошти на підвищення технічного рівня поліції.

Використання існуючих технологій і огляд перспективних технологій, що сприяють запобіганню злочинів.

МВС Великобританії активно співпрацює з правоохоронними органами та бізнесом з метою найбільш ефективного використання існуючих технологій для попередження та боротьби зі злочинністю. Основними напрямками роботи є:

- ***технології цифрової розвідки для запобігання злочинів***. Особливо великі можливості надає поліцейським розвідка за відкритими джерелами, в першу чергу по соціальним мережам і додатків. В умовах зниження віку злочинності, в тому числі повсякденному, вуличної, практично весь кримінал активно користується технічними пристроями. Витяг даних із захоплених в ході розслідувань ноутбуків або смартфонів дозволяє отримати результати, на які раніше, в доцифровому світі, у поліцейських йшли тижні наполегливої роботи. Починаючи з 2017 р. Міністерство внутрішніх справ приступає до реалізації програми «Цифрові розслідування і розвідка». Ця програма поряд із зусиллями щодо створення єдиної платформи заохочує оволодіння поліцейськими методами розвідки за відкритими джерелами і оснащення їх простим, але ефективним «софтом»;
- ***мобільні технології***. Міністерство створює у співпраці з британським бізнесом єдину систему зв'язку для аварійних служб, включаючи поліцію, пожежно-рятувальну службу і швидку медичну допомогу. Також ця система буде підключена до окремих бізнесових структур і громадських організацій.
- ***технології цифрового відео***. Британська поліція бачить три основні напрями використання цифрового відео в своїй діяльності: по-перше, це відеоматеріали з місця злочину; по-друге, це канал взаємодії з громадськістю; по-третє, це гігантський, поповнюваний в онлайн режимі відеоархів з камер спостереження в британських містах і на транспортних магістралях.

Вперше в історії у британській поліції є в розпорядженні програмно-апаратні засоби, що дозволяють в онлайн режимі працювати з потоковим багатоканальним відео. По суті, мова йде про те, що вперше у поліції

з'являється можливість предикативно аналізувати наміри потенційних злочинців.

Перспективні напрямки.

У МВС Великобритании Створений Центр перспективних прикладних наук и технологій (CAST). Его завдання є робота з бізнесом и наукою з виявлення нових технологій і при необхідності їх фінансова та інша підтримка. Особливу увагу Центр приділяє не міжнародним і провіднім Британським компаніям - постачальником МВС, а дослідницькім командам в британських університетах, стартапам и т. п. Центр не тільки уважно вивчає їх розробки, а й полегшує доступ кращим з них на тендери, що проводяться Міністерством внутрішніх справ .

В рамках роботи Центру поряд з традиційними напрямками особлива увага пріділяється таким перспективним технологіям, як:

- 3D и 4D-друк.
- дрони.
- біткойн і блокчейн-технології.
- загальний взаємозв'язок. В даний час світ рухається до суцільно пов'язаного середовища та інфраструктурі. До 2020 р в світі буде близько 20 млрд пов'язаних між собою мережевих пристроїв.

- цифрове шифрування.

Починаючи з 2013 р. багато британських громадян стали використовувати шифровану електронну пошту, месенджери і т. п. Це створює значні труднощі правоохоронним органам. Тому передбачається регламентувати можливості шифрування громадянами, а також спеціально передбачити обов'язок для виробників шифрованих комунікаторів надавати відповідні ключі правоохоронним органам.

3. Штучний інтелект і великі дані для запобігання злочинам.

Лідером впровадження штучного інтелекту в процес боротьби зі злочинністю є ФБР США. Основні роботи в цьому напрямку ведуться в Інформаційному центрі ФБР (NCIC). Це метабаза, що включає на початок 2017 року 21 базу даних, що містять досьє на 12 млн активних індивідуальних злочинців і членів злочинних організацій. В середньому NCIC відповідає на 14 млн запитів в день. Крім ФБР NCIC обслуговує більше 90 тис. точок доступу в органах кримінального правосуддя, а також судах, прокуратурі, системі виправних установ і т. п.

Інформаційний центр ФБР знаходиться в розпалі модернізації, відомої як проект N3G. В рамках проекту в систему включаються принципово нові блоки обробки і аналізу інформації, що базуються на інтелектуальному аналізі великих даних.

Основні напрямки застосування штучного інтелекту в структурі ФБР і поліції США в 2017-2020 рр.

Двосторонні та багатосторонні зустрічі, відкриті конференції та наради за зачиненими дверима дозволили визначити основні напрямки використання штучного інтелекту і його елементів в роботі ФБР і поліції штатів. Ці напрямки знайшли відображення в концепції N4G. У число основних

напрямків включаються такі.

1. Використання в аналітико-сітуаціонних центрах в офісах ФБР на місцях і аналогічних офісах поліції штатів програмно апаратного середовища з єдиною інтегральною обробкою файлів різної розмірності і формою подання, включаючи текстові, табличні, аудіо, відеофайли, сигнали від датчиків, банківські транзакції, показання локації і т. п.

Принципово від нині існуючих баз даних її відрізняють три обставини. Не людина, а машина буде приймати рішення про появу того чи іншого профілю в базі даних. Простіше кажучи, передбачається система, в корені відрізняється від нині прийнятого порядку. Зараз відповідні керівники поліції, агенти ФБР приймають рішення про заклад файлів на ту чи іншу людину. Як показує практика, ці рішення часто бувають помилкові і суб'єктивні. У новій системі передбачається забезпечувати нефільтрованими потоками інформації. Фільтрувати, а відповідно, визначати необхідність закладу профілів буде сама система. У систему вбудовується модуль глибоконавчаємих нейронних мереж. Даний модуль буде відповідати за своєчасне вилучення профілів і параметрів осіб, які за критеріями бази потрапили в неї, але в протягом певного часу не викликали інтересу з боку ФБР або поліції штатів.

Дана система на відміну від нині застосовуваних б де здатна взаємодіяти з кінцевими користувачами на природній мові і з використанням візуальних засобів.

2. Як уже зазначалося, одним з найбільш схильних до погроз з точки зору динаміки організованої злочинності секторів економічного життя є небанківські платіжні системи.

За погодженням з найбільш динамічними платіжними системами Stripe і Wise ФБР організувало підприємство по створенню і експлуатації платформи з виявлення шахрайств та зломів платіжних систем. Дана система буде відкрита для всіх ліцензованих платіжних систем. Передбачається, що вони будуть виділяти на утримання системи щорічний внесок в залежності від обсягу транзакцій і рівня сертифіката інформаційного захисту, присвоєного платіжній системі. Виробником системи в результаті тендеру вибрана компанія Palantir.

З використанням платформи контекстного інтелекту Nigel передбачається створити безпаперовий офіс агента ФБР або поліцейської дільниці.

Система Nigel на відміну від інших здатна не тільки до семантичного аналізу (розпізнавання об'єктів по онтології; онтології можуть бути різні - властивості, відносини, функції, людина, юридична особа, предмет і т. п.), а й до контекстного розпізнаванню ситуації. Ситуації можуть бути однакові по онтології, але різними за змістом. Наприклад, в двох ситуаціях беруть участь одні й ті ж персонажі - жінка, чоловік і дитина. Контексти ситуацій можуть бути різні. В одному випадку це може бути щаслива сім'я; в іншому - колишнє подружжя, що ділять дитини. Зараз жодна система, крім Nigel, не здатна розпізнавати ситуацію. В результаті система буде давати експертні

поради правоохоронцям, прив'язані до унікальної конкретній обстановці.

Величезні масиви різноманітної інформації, наприклад, інформація з форумів і соціальних мереж, відеозапису, текстові документи, логфайлів (англ .: log file - файл реєстрації) або, наприклад, дані про трафік і з'єднаннях абонентів, містяться в різних джерелах, нерідко за межами організації. В результаті правоохоронні структури можуть мати доступ до величезного обсягу даних з внутрішніх і зовнішніх джерел і не мати необхідних інструментів, щоб здійснити їхню спільну обробку, виявивши певні взаємозв'язки і зробити на їх основі значущі висновки.

Досвід співпраці компанії IBM з правоохоронними органами свідчить про те, що потрібні: по-перше, консолідація розрізнених джерел інформації в єдине сховище даних; по-друге, застосування спеціального програмного забезпечення, що дозволяє виявляти корисну інформацію із розрізнених і неповних задокументованих даних, а також з непов'язаних подій; використання спеціалізованих, програмно апаратних рішень, що максимально прискорюють роботу і прийняття рішень при обробці величезних обсягів даних структурованої і неструктурованої інформації.

З цією метою в Нью-Йорку в 2007 році було прийнято рішення про створення централізованого операційного центру громадської безпеки. Було інтегровано більше 100 розрізнених джерел даних. Всі потоки інформації від патрульних машин, тисяч камер відеоспостереження, дзвінки від свідків у вигляді неструктурованих даних надходять на корпоративну шину даних і перетворюються в універсальний формат. Потім аналітичні інструменти асоціюють інформацію, поміщаючи її в певний контекст, і розподіляють її відповідно до запитів користувачів. Аналітична система асоціювання розпізнає не тільки структуру, але і значення інформації, включаючи взаємини між різними частинами. Створення єдиного сховища дозволило знизити злочинність в місті на 27%.

Був реалізований також сервіс пошуку корисних даних з погано документованої інформації: скарг громадян, звітів поліції, записів на номер 911, протоколів арештів і ін. Всі ці дані рясніють неточностями, скороченнями, абревіатурами, спеціальними термінами і т. п., і виявлення потрібних відомостей і взаємозв'язків за допомогою традиційного контекстного пошуку в них вкрай утруднено.

В результаті вдалося досягти загального підвищення ефективності роботи. Застосування інструментарію пошуку та аналізу дозволило сформувати опис подій, класифікувати їх (при цьому пошук здійснюється по неструктурованою інформації, що містить часом неточні опису).

В цілому це дозволяє створити прості, уніфіковані уявлення для кожного аспекту роботи поліції, включаючи планування, звітність і спільну роботу.

У 2001 р. IBM придбала британську компанію **i2** Group, яка розробляла аналітичні засоби для правоохоронних органів, спецслужб, військової розвідки і фахівців з боротьби з «фродом» (англ .: fraud - шахрайство в сфері IT).

Один з продуктів, заснованих на i2, розроблений спеціально для поліції. Він дозволяє швидко отримати доступ до інформації, накопиченої правоохоронними органами, і проявити в ній приховані зв'язки між людьми, місцями, автомобілями, мобільними телефонами і тому подібними об'єктами.

У канадському Ванкувері поліція запровадила систему аналізу даних, засновану на розробках IBM і географічній інформаційній системі компанії ESRI. Система не тільки виявляла тенденції, але і пророкувала ймовірний час і місце скоєння злочинів. З 2007 до 2011 року кількість злочинів, пов'язаних з власністю, скоротилося на 24%, а насильницька злочинність - на 9%.

Схожі результати повідомляють поліцейські департаменти Лас-Вегас,

Мемфіса і інших міст, де експериментують з програмами для аналізу даних.

У Сіетлі він використовується для прогнозування збройного насильства.

У Кенті (Англія) система PredPol застосовувалася для передбачення наркозлочинів і грабежів. Поліція Кента була ще більш винахідливою: не тільки відправляла своїх співробітників патрулювати небезпечні райони, але також вдавалася до допомоги місцевих волонтерів дружинників і працівників реабілітаційних клінік для наркоманів.

Система прогнозування в режимі реального часу аналізує нові звіти про злочини в цих містах, і червоний квадрат, який прогнозує місце вчинення правопорушення, може зрушитися в будь-який момент. Хоча патрульні з підрозділів, що використовують PredPol, зобов'язані перебувати певну кількість часу в кожному з тих червоних квадратів, вони не просто сліпо слідують командам системи. Патрульний вправі приймати рішення самостійно, виходячи з обстановки, а не тільки підкорятися алгоритмам.

Використання великих обсягів даних і обробка за допомогою математичних моделей значно перевершують за кінцевим результатом банальне визначення гарячих точок на карті в ручному або навіть автоматизованому режимі. Спеціальні випробування, що проводилися майже два роки в трьох територіальних підрозділах лосанджелесской поліції, встановили, що PredPol вірно передбачає в два рази більше місць злочинів, ніж дозволяють кращі з існуючих методик.

Спеціальне програмне забезпечення застосовується поліцією Чикаго. Воно з високою ймовірністю пророкує не тільки імена майбутніх убивць, а й тих, хто стане жертвами, - в американській злочинному середовищі ці категорії людей щільно перетинаються.

Програма, розроблена за участю вчених з Іллінойського технологічного університету (США) (розробник - професор М. Веркік), дозволила поліції Чикаго визначити список осіб, які перебувають в групі ризику скоєння вбивств. Дізнавшись їх імена, поліцейські ведуть з ними профілактичну роботу, імовірно що дозволяє знизити ймовірність зазіхань на життя інших людей.

За заявами поліції, новий алгоритм є досить ефективним. З 2,7 млн жителів Чикаго він відібрав лише 1400 осіб, що мають надзвичайно високу

ймовірність убити або бути убитим.

Понад 70% членів даного списку були застрелені протягом 2016 р. Кожен четвертий стрілок також входив в список Департаменту поліції Чикаго. Згідно з даними правоохоронців 117 з 140 осіб, заарештованих під час загальноміського рейду проти банд, також були присутні в вищезазначеному переліку і становили «групу ризику».

Поліцейські застосовують новий метод не тільки для своєчасного здійснення арештів. Влада міста бачать в алгоритмі ефективний засіб «персональних повідомлень», в яких працівники соціальної сфери та громадські лідери агітують членів - лідерів «Списку стратегічних суб'єктів» змінити спосіб життя і назавжди покинути кримінальний світ.

Поліція міста Дарема на півночі Англії запустила в 2017 р. комп'ютерну програму, яка за допомогою алгоритму штучного інтелекту повинна допомогти поліцейським визначити, кого слід утримувати під вартою, а кого можна відпустити. Алгоритм класифікує затриманих за ступенем ризику - з якою ймовірністю вони можуть знову вчинити злочин.

Програма Harm Assessment Risk Tool (Hart) «вивчала» дані поліції Дарема про арешти за п'ять років, між 2008 і 2012 рр. Потім система була протестована Даремського поліцією в 2013 р., після чого протягом двох років вивчалися результати цього тестування - поліцейські відстежували, чи повернулися звільнені до злочинного життя чи ні. Як з'ясувалося, алгоритм зміг передбачити, що затриманий не представляє небезпеки, в 98% випадків. А що знаходяться в групі «високого ризику» комп'ютер правильно виявляв в 88% випадків.

Програма може бути хорошим помічником у багатьох випадках: коли поліції слід вирішити, чи тримати затриманого ще кілька годин; чи слід відпустити його під заставу до того, як йому будуть пред'явлені офіційні звинувачення, і чи варто тримати його під. арештом після пред'явлення звинувачень.

Крім того, британська поліція з 2014 р. перевіряє комп'ютерну систему, яка може зібрати воєдино те, що могло статися на місці злочину. Ідея полягає в тому, що система, яка називається VALCRI (Visual Analytics for Sensemaking in Criminal Intelligence Analysis), зможе протягом декількох секунд виконувати копітку роботу аналітика, звільняючи час для того, щоб зосередитися на ділі, а також провокуючи нові напрямки розслідування і можливі упущені деталі.

Основна робота VALCRI полягає в тому, щоб допомогти генерувати правдоподібні ідеї про те, як, коли і чому було скоєно злочин, а також хто зробив це. Система сканує мільйони поліцейських записів, інтерв'ю, фотографій, відеороликів та багато іншого, щоб визначити зв'язку, які мають відношення до справи. Все це потім представлено на двох великих сенсорних екранах для взаємодії з аналітиком.

Мідлсекський університет є одним з декількох вищих навчальних закладів, які в даний момент задіяні в розробці системи VALCRI.

Найвідомішою компанією, що спеціалізується на прогнозуванні

злочинів, є Palantir Technologies, що вийшла на комерційний ринок з тіні спецслужб.

Розроблене Palantir спеціалізовані рішення здатні зібрати воєдино найрізноманітнішу інформацію (дані ДНК, записи систем відеоспостереження і телефонних переговорів), відстежувати пересування по номерним знакам орендованих машин і багато іншого.

Механізм дії цього програмного забезпечення полягає в аналізі персональних даних та виявленні транзакцій, які завжди йдуть в тісній зв'язці з паттернами, які супроводжують ті чи інші злочини. Іншими словами, у спецслужб є значні масиви даних, серед яких відомості про фінансові операції, відбитки пальців і зразки ДНК, плани будівель і топографічні карти, дані радіоперехоплення, «гарячі» новини зі ЗМІ, повідомлення інформаторів, інформація з соцмереж і ін.

Програмне забезпечення Palantir вже допомогло розкрити злочинну мережу, яка готує теракти в декількох країнах світу. Його також використовували в Афганістані для прогнозування атак моджахедів.

Крім того, рішення Palantir дозволило виявити членів мексиканського наркокартелю, які вбили співробітника митної служби США, а також дозволити множина не таких гучних, але не менш важливих випадків, в тому числі знайти педофіла в Нью-Йорку вже через годину після нападу на дитину, виявивши його на відеозаписах з камер поліцейського управління.

Департамент поліції Нью-Йорка разом з Microsoft розробив Domain Awareness System (DAS) - систему, яка агрегує і аналізує інформацію про громадську безпеку зі звітів, камер спостереження, спостережень очевидців і т. д. Потім цю інформацію про потенційні загрози і кримінальну активність в режимі реального часу отримують слідчі і аналітики департаменту.

Схожим чином працює ShotSpotter - акустична система спостереження, яка фіксує постріли зі зброї і оповіщає обетом поліцію. Сенсори ShotSpotter дозволяють визначити місце, де стався інцидент, з точністю до двох футів.

Дана технологія використовується вже в 75 містах США.

Іншою частиною тренда в використанні нових технологій для підвищення обізнаності є використання соціальних медіа і, зокрема, Twitter. Поліція все частіше покладається на цю соціальну мережу і використовує для комунікації з жителями міста.

Наприклад, під час заворушень, влаштованих спортивними вболівальниками у Ванкувері (Канада), поліція використала Twitter для того, щоб бути в курсі ситуації, а після того, як заворушення були усунені, Twitter і Facebook стали каналами, через які свідки могли повідомити поліції наявну у них інформацію.

Поліція Берліна розглядає можливість установки програмного забезпечення, яке зможе передбачати злочини, майже як показано в науково-фантастичному фільмі «Особлива думка». Навіть проект носить таку ж назву«Precobs», як у фільмі.

Розроблена німецькою фірмою програма передбачає, де і коли з найбільшою ймовірністю відбудеться злочин.

Потрібно сказати, що схожі програми вже кілька років успішно працюють в декількох американських містах. Наприклад, в 2011 р. Сантакрус (штат Каліфорнія) першим в світі впровадив математичну модель розрахунку ймовірності злочинів, яка кожен день встановлює новий маршрут для патрульних машин, ґрунтуючись на статистиці злочинів по вулицях. Враховуються день тижня, час доби, наявність/відсутність трансляції футбольних матчів по телебаченню і інші фактори.

Патрульні поліцейські Сантакрус кожен день отримують новий маршрут для патрулювання із зазначенням 10 гарячих точок маршруту. Ось як виглядає ця інформація в інтерфейсі Google Maps:

для кожного квадрата розміром 150 на 150 м вказується ймовірність скоєння злочину в 24-годинний період, розподіл цієї ймовірності за двома видами злочину (автомобільні і домашні), час початку двох найнебезпечніших часових інтервалів.

Німецька програма PreCrime Observation System працює приблизно за таким же принципом, обчислюючи ймовірність скоєння злочинів з тих чи інших координатах з урахуванням минулого статистики.

Поліція Амстердама поставила завдання розробити програмний продукт, який міг би автоматично систематизувати тисячі поліцейських звітів, відбираючи ті, що мають відношення до торгівлі людьми. Система повинна була не просто відбирати підозрілі випадки, а знаходити закономірності, встановлювати коло людей, можливо причетних до злочинного бізнесу, тобто виявляти і ідентифікувати потенційних підозрюваних.

В ході роботи фахівці проаналізували близько 70 тис. поліцейських звітів, складених з 2008 р. В основному це були звіти патрульних поліцейських, які проводили огляд автотранспорту або патрулювали вулиць Амстердама. Лише приблизно в тисячі випадків поліцейським було відомо, що мова дійсно йде про осіб, що мають відношення до торгівлі людьми.

Всі індикатори (їх можна виявити в тексті автоматично) розділили на групи:

- статичні ознаки (національність, проблеми з документами, велика сума готівки, жінки не розмовляють, документи жінок перебувають у водія, повії, насильство, сліди насильства);
- змінювані ознаки (район «червоних ліхтарів», дорога машина, жінки в машині, торгівля в машині, канікули, регулярне відвідування сумнівних клубів, регулярна доставка дівчат в клуб);
- ознаки соціального оточення (людина була помічена з підозрюваним чи відомим злочинцем, сама була під підозрою).

Також індикатори поділялися на ранні і пізні, тобто можливі і явні, сильні ознаки, відповідно. Виділені ознаки заносилися в таблицю. Дивлячись на неї, можна було визначити, скільки підозрілих ознак є в тому чи іншому звіті. Поліцейські при складанні звіту перерахували такі індикатори, як «дорога машина», «проблеми з документами», район, де працюють повії.

Звіт, що містить слова-індикатори, вимагав більш пильної уваги

правоохоронних органів. Щоб виявити і ідентифікувати осіб, причетних до торгівлі людьми, поліцейські аналізували формальні поняття.

Розроблений інструмент дозволив поліцейським в інтерактивному режимі за допомогою таблиць формальних понять виділити ряд ознак і виявити потенційних підозрюваних.

Компанія Fujitsu Laboratories Ltd спільно з Університетом електрокомунікацій (Японія) розробила алгоритм для піймання злочинця в місті. Алгоритм заснований на теорії ігор, яка математично описує технологію захисту і нападу як технологію для прийняття рішень.

Японське міністерство, яке контролює митницю, в 2017 р. почало польові випробування ШІ і дронів для боротьби з контрабандою, плануючи повністю впровадити таку технологію напередодні Олімпійських ігор 2020 р.

В даний час митні інспекції в аеропортах і гаванях проводять візуальну перевірку рентгенівських знімків для виявлення контрабанди наркотиків і вибухових речовин. На додаток до візуальних оглядів Міністерство фінансів Японії планує використовувати ШІ. З його допомогою будуть проаналізовані вже наявні в базі даних зображення, щоб допомогти виявляти контрабанду в рентгенівських зображеннях.

Також будуть піддані аналізу дані митниць про в'їзд і виїзд людей з Японії, про експорт та імпорт вантажів, щоб визначити, коли виникає висока ймовірність провезення контрабанди.

Особлива активність в роботах зі створення ШІ спостерігається в **КНР**. Перша в Китаї національна лабораторія по розробці технології «мозкоподібного» ШІ 13 травня 2017р. відкрилася в місті Хефей, що є адміністративним центром провінції Аньхой (Східний Китай). Створення цієї лабораторії було затверджено Державним комітетом у справах розвитку і реформ КНР. Вона базується в Китайському науково-технічному університеті і націлена на розвиток парадигми «мозкоподібних» обчислень і їх додатків.

Даний університет відомий своїм провідним статусом в розробці технології квантового зв'язку, він розміщує національну лабораторію у співпраці з провідними китайськими науковими установами, включаючи Університет Фудань і Шеньянський інститут автоматизації Академії наук Китаю, а також оператора найбільшого в Китаї сервісу інтернет-пошуку - Baidu.

У Росії також використовують в попередженні злочинності і тероризму новітні технології, що використовують ШІ і великі дані.

Наприклад, основною автоматизованою інформаційно-пошуковою системою (АІПС) ОВС на транспорті є програмно-технічний комплекс (ПТК)

«Розыск Магистраль». Цей комплекс почав впроваджуватися в оперативно- службову діяльність в 2000 р. Він призначений для виконання в автоматизованому режимі наступних функцій:

- виявлення в пасажиропотоку осіб, які перебувають у розшуку, а також осіб, що представляють оперативний інтерес для правоохоронних органів, за допомогою автоматичного порівняння баз даних по особам, які

перебувають у федеральному і місцевому розшуку, осіб, які мають оперативний інтерес, втрачених і викрадених документів і т. Д . з транспортними базами даних;

- цілодобового поповнення баз даних інформацією, що надходить з ВАТ«РЖД», його філій і структурних підрозділів; підприємств авіатранспорту; ДІАЦ МВС Росії; інформаційних центрів МВС, ГУМВС, УМВС, УВСТ; підлеглих лінійних підрозділів та інших правоохоронних органів;
- надання можливості пошуку по базах даних АІПС в різних режимах;
- вивантаження даних з інформаційних масивів АІПС і їх передачі до вищестоящих підрозділи для формування загальноросійського (міжрегіонального) інформаційного масиву;
- здійснення за запитом користувача аналітичної обробки наявної в базах даних ПТК інформації з метою виявлення і розкриття злочинів у сфері пасажирських перевезень;
- проведення аналітичних розробок по реєструється злочинів і справах оперативного обліку;
- формування статистичної звітності про результати роботи системи як по виявленню осіб, які перебувають в розшуку і представляють оперативний інтерес, так і за кількістю та якістю виданої інформації за запитами користувачів.

В основу роботи аналітичних модулів закладений принцип галузевої інтеграції інформації. Для кожного напряму роботи (по лінії карного розшуку, боротьби з незаконним обігом наркотиків, боротьби з організованою злочинністю і ін.) існує свій АРМ, що дозволяє за допомогою спеціально розроблених алгоритмів витягувати із загального банку інформацію та аналізувати дані, необхідні для виявлення і розкриття конкретних видів злочинів .

Для інформаційної підтримки нарядів патрульно-постової служби і оперативних співробітників служать мобільні термінали ПТК

«РозискМагістраль». Ці термінали являють собою кишенькові персональні комп'ютери і призначені для оперативного доступу співробітників правоохоронних органів до інформації баз даних федерального і регіонального рівнів, таких як «Розшук осіб», «Паспорти», «Зброя», «Угон» та ін.

Систему «Штучний інтелект на кордоні», яка охороняє російсько-казахстанський кордон в межах Челябінської області, з 2016 р. тестують розробники. Розробником системи «Штучний інтелект на кордоні» є Об'єднана приладобудівна корпорація. Кілька комплектів системи готують під установку на далекосхідних, південних ділянках рубежів Росії.

Фіксацією порушень займаються безпілотники, інфрачервоні датчики, сейсмосенсори, радіолокаційні пристрої, а передана ними інформація узагальнюється комп'ютерною системою з інтелектуальною програмою. Напрацювавши базу даних, програма починає прогнозування небезпеки.

Стоїть завдання сухопутні ділянки державного кордону Росії оснастити інтелектуальною системою, здатною автоматично збирати і аналізувати інформацію про порушення рубежів країни. Завдяки цьому прикордонники в дистанційному режимі контролювати ситуацію на кордоні.

На морських напрямках продовжиться нарощування можливостей системи автоматизованого технічного контролю за надводною обстановкою.

На сухопутних ділянках кордону застарілі технічні засоби охорони кордону будуть планово замінені на сучасні зразки. При цьому стратегічною метою технічної політики стане послідовний перехід підрозділів до дистанційного контролю за охоронюваними ділянками державного кордону з одночасним скороченням використання особового складу для їх фізичної охорони.

Йдеться про рухомі і стаціонарних комплексах технічного спостереження нового покоління з прихованим (практично невидимим) розташуванням на місцевості. Контролювати обстановку на віддалених і важкодоступних напрямках будуть БПЛА.

Крім того, російські програмісти розробили систему, яка в цілях контролю за оперативною ситуацією автоматично взаємодіє з різними технічними засобами охорони: відеокамерами, інфрачервоними і сейсмічними датчиками, радіолокаційними станціями та безпілотниками, що фіксують факти порушення. Вона не тільки призначена для збору різноманітної інформації, але і містить елементи ШІ. Це дозволяє прикордонникам провести аналіз і прогнозування ситуації, виробити готові пропозиції по охороні кордонів, прорахувати дії і маршрут порушників, а також заходи, необхідні для припинення дій зловмисників, з оцінкою можливих ризиків. При цьому враховуються реальні умови місцевості, статистика порушень, погодні умови, розташування прикордонних постів і нарядів і багато інших чинників.

Система повністю базується на вітчизняних програмних рішеннях, які гарантують захист інформаційних ресурсів від витоку даних, хакерських атак, інших сторонніх втручань.

Дані комплекси пройшли позитивну апробацію в Кабардино-Балкарії, КарачаевоЧеркесії, Північній Осетії та Інгушетії.

Використання штучного інтелекту, великих даних і квантової криптографії для попередження фінансових шахрайств.

Аналітичний підрозділ Microsoft по боротьбі зі злочинами в сфері високих технологій Digital Crimes Unit (DCU) було створено в листопаді 2013 р. Великі дані виступають тут в ролі ультимативного інструменту розслідування і запобігання кіберзлочинів. Впроваджуючи чергову схему, зловмисники всюди залишають цифрові сліди. Окремо ці малі зміни зазвичай ігноруються. Однак на рівні великих даних злочин з використанням мережевих технологій виглядає як характерний патерн. Повністю приховати його не вдасться, як би ретельно не маскувалися окремі прояви.

Стало набагато легше відстежити нелегальні ключі активації програмних продуктів. Раніше самі розробники виявляли тільки вкрадені

одно-користувацькі ліцензії, коли їх намагалися одночасно використовувати кілька людей. Зараз обмін даними дозволяє побачити, що корпоративний ключ однієї з програм був вкрадений або відбувається перевірка генератора ключів.

За допомогою візуалізації великих обсягів спільних даних можна бачити незвичайні сплески активності на серверах реєстрації, що може вказувати на тестування вкрадених або згенерованих ключів. Без засобів візуалізації ці аномалії, швидше за все, залишалися б непоміченими.

Сьогодні на технологіях аналізу великих даннях Microsoft створює цілу інфраструктуру для запобігання будь-якої нелегальної мережевої активності.

Більшість мережевих атак і розсилок спаму виконуються з заражених комп'ютерів, які формують бот-нети. Визначення їх складу і керуючих серверів

- важливе завдання забезпечення глобальної інформаційної безпеки. У цьому напрямку працюють компанії «Доктор Веб» і «Лабораторія Касперського».

Застосовуючи технології аналізу великих даних, в Microsoft розробляють алгоритми, що спрощують визначення керуючих серверів і перехоплення контролю над ними. Також провайдери попереджаються про те, що комп'ютери їхніх абонентів заражені. Така співпраця допомагає дізнатися додаткові деталі про мережеву активність і обчислити подальші кроки злочинної групи.

Корпорація IBM оголосила, що пристосувала самонавчальний суперкомп'ютер Watson, здатний працювати з інформацією на природній мові, для використання в сфері інформаційної безпеки.

Фахівці IBM і дослідники з восьми американських університетів планують завантажити в самонавчающуся систему вміст бібліотеки XForce, яка включає матеріали, що охоплюють два десятиліття досліджень в сфері інформаційної безпеки, детальну інформацію про 8 млн спамерських та фішингових атак і опису більше 100 тис. вразливостей.

Передбачається, що після завершення навчання Watson буде оперативно збирати і зіставляти загальнодоступні відомості про нові загрози, в тому числі інформаційні бюлетені, статті, звіти компаній, відео, навіть публікації в блогах.

Він буде в курсі всього, що відбувається, і за рахунок цього зможе самостійно пізнавати проблеми і пропонувати рекомендації щодо їх вирішення.

У IBM виходять з припущення, що потік інформації про загрози якщо ще не перевищив людські можливості, то неодмінно це зробить. Національна база даних вразливостей вже на цю година містить більше 75 тис. записів і швидко росте. Щороку публікується близько 10 тис. дослідницьких робіт, так чи інакше пов'язаних з інформаційною безпекою, і більше 60 тис. постів в блогах на ту саму тему. Watson здатний проаналізувати їх всі. Люди - ні.

Нова система боротьби з комп'ютерним шахрайством на основі великих даних була розроблена в компанії Visa. На відміну від попередників

вона враховує до 500 особливостей кожної транзакції і аналізує те, що відбувається з точністю до окремих банкоматів. За рік система зупиняє шахрайські платежі на суму приблизно 2 млрд дол. США в рік.

Один з великих американських банків підключив до боротьби з шахраями розроблений в IBM суперкомп'ютер Watson.

Система IBM, яка використовує елементи Watson, аналізувала потік транзакцій в реальному часі, оцінюючи підозрілість кожної з них. На оцінку, серед іншого, впливала історія відносин банку з торговою точкою, яка ініціювала угоду. Чим більше шахрайських транзакцій в її послужному списку, тим менше до неї довіри.

У IBM стверджують, що система на 15% збільшила кількість виявлених шахрайських звернень до банку і на 50% скоротила число помилкових спрацьовувань. При цьому сума, яку вдалося захистити від шахраїв, зросла на 60%.

Ті ж методи працюють і в інших областях, причому не менш дієво. Міністерство праці Німеччини пристосувало їх для аналізу заявок на одержання допомоги по безробіттю. Скоро стало ясно, що близько 20% посібників виплачувалося незаслужено. Таке застосування великих даних дозволили міністерству скоротити витрати на 10 млрд євро.

Американська Комісія з цінних паперів і бірж (SEC) теж автоматизувала пошук шахраїв, але в даному випадку мова йде не про дрібні жуликів, конвертаційних крадені кредитки, і навіть не про фальшиві безробітних. В SEC мітять вище і виводять на чисту воду мегакорпорації, які вчиняють фінансові порушення.

Поява великих обсягів інформації дозволила зробити важливий крок на шляху до створення програм захисту, які дозволяють перехоплювати 60-70% вірусів, що залишилися непоміченими традиційним антивірусним «софтом». Машини, що навчаються, дозволяють виявити ДНК вірусних сімейств, а не просто окремі віруси.

Цей підхід був запозичений зі світу даталогії, або науки про дані, і виявився дуже результативним завдяки величезній базі, швидко зібраної компаніями, які почали відстежувати поведінку заражених вірусами комп'ютерів. Автоматизація виявлення таких аномальних кроків необхідна тому, що людина або навіть велика група людей не зможе виявити їх досить швидко.

Центр з обміну та аналізу інформації про фінансові послуги - впливова організація з кібербезпеки у фінансовій сфері - оголосив у жовтні 2016 року про створення підрозділу, метою якого є боротьба з кіберзлочинністю і зміцнення кібербезпеки фінансових інститутів. Як повідомили в FSISAC, створення цього підрозділу - результат переговорів восьми банків (Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street і Wells Fargo).

Функції самого Центру з обміну та аналізу інформації про фінансові послуги приблизно такі ж, але він об'єднує 7 тис. банків. У зв'язку з цим великі фінансові інститути вирішили, що їм необхідно виділитися в окрему

групу, тому що хакери в першу чергу атакують саме їх, а не більш дрібні банки. Новий підрозділ, який називається Центром з фінансового системного аналізу та стійкості, також координуватиме діяльність банків і американського уряду в цій сфері.

Про можливості захисту інформації в сучасних організаціях за допомогою квантової криптографії зробив доповідь А. Львівський на міжнародній конференції «Вперед в майбутнє: роль і місце Росії», приуроченої до 175-річчю Ощадбанку.

Протиборство між кіберзлочинцями і кіберполіцейських йде давно - на кожен новий більш витончений метод захисту придумують нові методи злому. До сих пір боротьба йшла в сфері математики і кібернетики - створювалися нові криптографічні алгоритми, нові методи дешифрування, нові програми для злому, нові віруси. Але вже близько час, коли на поле битви вийде фізика і це буде квантова фізика.

Звичайні методи шифрування мають одне непереборне слабке місце - учасникам розмови потрібно обмінятися ключами шифру.

Користуватися звичайною лінією зв'язку для передачі шифру можна: якщо зловмисник цю лінію прослуховує, всі зусилля щодо шифрування пропадуть дарма. Тому найбільш важливі криптографічні шифри, які використовуються для передачі цілком таємних державних або військових донесень, посилають зі спеціальними охоронюваними кур'єрами. Такий спосіб, природно, надзвичайно дорогий.

Тому для повсякденних застосувань, таких як передача номера кредитної картки з комп'ютера користувача на сервер при інтернет-шопінгу, використовують криптографічні системи з відкритими ключами, засновані на несиметричності деяких математичних операцій. Наприклад, звичайному комп'ютеру для розкладання відкритого ключа довжиною 2 кілобита буде потрібно кілька сотень років. Так влаштований, зокрема, широко застосовуваний алгоритм RSA.

Але дуже скоро такі системи шифрування виявляться марними, з'явиться інструмент, здатний зламувати їх за кілька хвилин, - квантовий комп'ютер. Поки справжні квантові комп'ютери, що складаються з десятків кубітів, ще не створені. Дуже складно утримати кубіти в певному стані тривалий час. Поки кращого результату тут домоглася IBM, яка за допомогою квантового комп'ютера з п'яти кубітів змогла розкласти на множники число 15. Канадська компанія DWave випускає квантові комп'ютери з тисячі кубітів, з якими експериментують в Google і NASA. Однак машина DWave - не універсальна квантовий комп'ютер, і її перевага в порівнянні з класичними комп'ютерами багатьма заперечується.

Навіть коли універсальні квантові комп'ютери будуть створені, вони підійдуть не для всіх обчислювальних задач. Однак вони мають колосальну перевагу перед класичними комп'ютерами в цілому ряді застосувань, багато з яких надзвичайно важливі.

Універсальні квантові комп'ютери можуть зробити революцію в сфері обробки великих даних, тобто методах виокремлення прихованих

закономірностей і зв'язків з великих масивів даних. Вони, наприклад, зможуть оцінювати закономірності споживчої поведінки і пропонувати товар більш точно підібраній аудиторії, вишукувати дані про терористів у величезних масивах «цифрових слідів».

Однак воістину «вибуховий» характер, що визначив технологічну гонку в цій області, носить саме здатність квантового комп'ютера швидко розкладати числа на множники, тобто зламувати криптографічні системи з відкритими ключами. Саме це робить квантовий комп'ютер зброєю в кібервійни - атомною бомбою XXI ст.

Хоча до створення повноцінних квантових ЕОМ ще від 10 до 20 років, фахівці з кібербезпеки дуже серйозно сприймають цю потенційну загрозу.

Американське АНБ в січні 2016 р. випустило попередження і назвало криптографічні алгоритми, які потенційно можуть витримати квантову атаку.

Порятунок від квантових хакерів може принести квантова криптографія. Захищені канали зв'язку, які використовуються, наприклад, для транзакцій з кредитними картами, засновані на застосуванні ключів - кодів для зашифровування і дешифрування повідомлень. Квантова криптографія - це спосіб використовувати закони квантової фізики, щоб забезпечити безпеку передачі ключів.

Унікальна властивість квантової криптографії - це її здатність фіксувати будь-яку спробу підслухати інформацію при передачі.

Боротьба з біткойн-злочинністю та використання технології блокчейн для попередження злочинів.

З 2016 року Європол, Інтерпол і Базельський інститут управління домовилися про створення спільної робочої групи, що спеціалізується на цифрових валютах.

У завдання групи входить збір і аналіз інформації про злочинне використання цифрових валют, розслідування питань про зберігання доходів, одержаних злочинним шляхом, організація щорічних семінарів і зустрічей представників трьох відомств та інших установ, а також створення мережі фахівців з біткойн-злочинності.

Одночасно нью-йоркський стартап Chainalysis і Європейський центр Європолу з боротьби з кіберзлочинами підписали угоду про співробітництво та обмін даними, щоб протистояти онлайн-злочинам.

Постійно розкриваються факти використання криптовалюти в кримінальних цілях, що підривають довіру до неї у багатьох добропорядних громадян.

У липні 2017 року в США заочно звинуватили затриманого в Греції росіянина А. Винника в організації схеми з відмивання більше 4 млрд дол. США через популярну біткойнбіржу BTCe. За даними американського Мін'юсту, Винник не тільки створив біржу, але і був причетний до злому її більш популярного конкурента Mt. Gox.

Згідно з даними декількох американських відомств росіянин був засновником біржі BTCe і, як стверджується в обвинувальних документах, керував нею з 2011 р., дозволяючи злочинцям усього світу відмивати доходи

в декількох криптовалютах: крім біткойнів їм були доступні операції з Litecoin, Namecoin, Novacoin, Peercoin, Ethereum і Dash, а також їх переклади в долари, євро і рублі.

У заяві Мін'юсту США значиться, що Винник «вів бізнес значного масштабу» в США, хоча представляє біржу компанія зареєстрована на Кіпрі, а на сайті біржі зазначено, що її офіс знаходиться в Болгарії.

В цілому через BTCe було відмито понад 300 тис. біткойнів і десятки тисяч одиниць інших криптовалют, а серед її клієнтів було чимало американців. Саме тому одним з перших обвинувальних пунктів стало відсутність реєстрації компанії в Міністерстві фінансів США.

Крім того, Мін'юст вважає, що Винник знехтував боротьбою з відмиванням грошей: майданчик був популярним місцем для виводу коштів, виручених в результаті продажу наркотиків, зброї, викупів за хакерські атаки та іншу нелегальну діяльність.

У зв'язку з цим росіянину також пред'явлені звинувачення в змові з метою відмивання грошей і в легалізації злочинних доходів. Клієнтам біржі надавалася максимальна анонімність: незалежно від суми адміністрація не вимагала підтвердження особи і не обтяжувала користувачів зайвими формальностями.

Колегія присяжних суду Сан-Франциско вже затвердила обвинувачення, а Управління по боротьбі з фінансовими злочинами Мінфіну США призначило біржі BTCe штраф в розмірі 110 млн дол., а особисто Виннику - 12 млн дол. США.

За даними статистичного сервісу Bitcoinity, за останній місяць перед арештом Винника на BTCe прийшлося 3,73% від загальносвітового обсягу транзакцій - це понад 177 тис. біткойнів, що еквівалентно 444 млн дол. США, або 26,5 млрд руб.

Чимала частина цих коштів пройшла через біржу з використанням біткойнміксеров (сервісів для розбивки великих транзакцій на більш дрібні, щоб їх не можна було відстежити по блокчейну), після чого була обміняна на звичні валюти - долари і євро. Гроші виводили великі постачальники і торговці наркотиками, що переважно проводили справи в біткойнах, які зіткнулися з загрозою втрати грошей внаслідок потенційного розгалуження крипто валюти**.**

Chainalysis спеціалізується на ідентифікації зловмисників, відстежуючи їх дії в блокових ланцюгах. Команда розробників стартапу працює над програмою, яка буде дотримуватися конфіденційності клієнтів і в той же час запобіжить злому системи.

Конфіденційність інформації заважають банкам обмінюватися інформацією про здійснювані ними транзакції, що дозволяє недобросовісним клієнтам використовувати одні і ті ж документи багаторазово. Саме тому технологія блокчейн, що гарантує прозорість усіх транзакцій, могла б стати вирішенням проблеми інвойс-шахрайства.

Але впровадження блокчейна зніме проблему шахрайства тільки в тому випадку, якщо перейти на розподілену ланцюг вирішиться відразу

більшість банків.

5. Використання для запобігання терористичних актів технологій, що дозволяють бачити крізь стіни.

Що сьогодні відомо про технології, які допомагають бачити крізь стіни?

1. Зворотнорозсіяне рентгенівське випромінювання (ЗРРВ) - технологія, при якій рентгенівські промені від джерела тривка крізь об'єкт, а відображаються. Так як об'єкт не треба просвічувати наскрізь, можливо використовувати випромінювання з інтенсивністю на кілька порядків нижче, ніж при проникаючому випромінюванні.

До числа речовин з малою атомною масою належать вибухові і наркотичні речовини, спиртовмісної рідини, тканини тіла людини. Це дозволяє легко ідентифікувати приховані органічні матеріали або людей, які можуть становити загрозу безпеці.

Використання технології ЗРРВ дозволяє:

- отримувати зображення органічних предметів, погано розрізняються при зазвичай використовуваної технології проникаючого рентгенівського вивчення;
- розміщувати джерело і приймачі випромінювання в пристроях огляду, розташованих з одного боку об'єкта, який оглядають — створювати за рахунок малої потужності випромінювання пристроїв, що використовують дану технологію, системи, безпечні для операторів і людей.

2. Вчені навчилися бачити людей через стіни за допомогою WiFi.

Компанія Technische Universität Ilmenau (ФРН) створила в 2017 р. унікальний високочутливий компактний прилад, який дозволяє з високим ступенем деталізації дивитися крізь перешкоди. Розробники пристрою стверджують, що він дає можливість заглянути за бетонні і цегляні стіни навіть багатометрової товщини. Фахівці компанії переконані, що їх «всевидюче око» допоможе в поліцейських і рятувальних операціях, а також в боротьбі з тероризмом.

Фізики з Массачусетського технологічного інституту (MTI) придумали в 2016 р., як за допомогою звичайного WiF-передатчіка бачити людей крізь стіни, причому не просто бачити, а й навіть визначати вагу і зріст людини. Вчені впевнені, що нова технологія знадобиться спецслужбам та правоохоронним органам.

6. Глобальна навігаційна система і електронне стеження з метою запобігання злочинам та актів тероризму.

Глобальна навігаційна система - це сукупність методів, програмних і технічних засобів, що дозволяють організувати фіксацію просторово-часової інформації та отримання її правоохоронними органами. Метою створення даної системи є підвищення рівня інформаційно-аналітічного забезпечення діяльності правоохоронних органів при здійсненні розслідування та попередження злочинів.

Комплекс засобів отримання просторово-часової інформації включає в себе наступні підсистеми: ГЛОНАСС, підсистему стаціонарного зв'язку, підсистему мобільного зв'язку, підсистему радіочастотної ідентифікації, підсистему відеофіксації, підсистеми фіксації фактів обігу та персоналізації.

Для забезпечення оперативності отримання просторово-часової інформації про контрольовані об'єкти, а також подання даної інформації в зручному для візуального сприйняття вигляді необхідна інтеграція систем з автоматичною фіксацією даних в єдину структуру. Основою для даної інтеграції можуть служити існуючі програмно-технічні комплекси систем моніторингу транспортних засобів, що функціонують на основі супутникової навігації, яка дозволяє отримувати інформацію про контрольованих об'єктах у вигляді карти із зазначенням їх місцезнаходження в певний момент часу. Одночасне відображення на карті місцевості просторово-часової інформації з усіх систем з автоматичною фіксацією даних дозволяє провести попереджувальні заходи по припиненню злочинів.

В єдиному комплексі з глобальної навігаційної системою слід розглядати і нові технології електронного контролю.

Після подій 11 вересня 2001 р створено ряд цікавих *технологій дистанційного стеження*, які можуть знайти повсюдне застосування.

Після ліквідації У.бенЛадена командою американського спецназу SEAL Team6 в поле зору журналістів потрапила секретна програма Пентагона під назвою «Мітки, відстеження і пошук», або TTL. Метою цього проекту є створення засобів, які дозволяють вистежити особливо важливих осіб, які переховуються в районі бойових дій або навіть серед населення іншої країни.

В даний час арсенал засобів стеження охоплює практично всі можливі способи ідентифікації та супроводу людини: від класичних сканерів відбитків пальців і райдужної оболонки ока до теплової сигнатури конкретної людини і мікроскопічної пилу, розпилюється з безпілотних літаків і світиться в променях радарів.

Квантова точка на карті.

Щоб відстежувати пересування певної людини і виділяти його з натовпу, американські військові розробляють спеціальну рідину, яка дозволяє виявити об'єкт з великої відстані.

Компанія Voxtel розробляє продукт під назвою NightMarks. Він являє собою прозору рідину, що складається з крихітних нанокристалічних квантових точок на основі селеніду кадмію.

Цей матеріал здатний поглинати ультрафіолетове (200-400 нм) або інфрачервоне (700-1600 нм) випромінювання, а потім ефективно передавати енергію на спеціальні нанокристалічні люмінофори, які світяться як у видимій (400-700 нм), так і в ближній інфрачервоній області спектра .

Досить нанести таку рідину на одяг або шкіру людини (простим рукостисканням, за допомогою БПЛА або іншим способом), і безпілотний розвідник зможе надійно відслідковувати яскраву мітку з великої відстані. Ефектами поглинання і випускання світла можна управляти, що дозволяє

змінити оптичні властивості квантових точок і створити безліч своєрідних спектральних штрихкодів. Таким чином, з'являється можливість відстежувати і надійно ідентифікувати безліч об'єктів.

Використання RFID-чіпів.

Вони схожі на ті, що застосовуються для мітки товарів в магазинах. В даний час армія США вже широко використовує цю технологію ідентифікації своїх сил на полі бою і логістики.

Фахівці Sandia National Laboratories розробили RFID-мітки, які здатні реагувати на радіолокаційний імпульс і з високою точністю визначати місце розташування об'єкта стеження. Наприклад, звичайні чіпи, які використовуються в магазинах, мають дальність дії в кілька метрів, в той час як RFIDметкі від Sandia мають радіус до 20 км. Особливістю технології є висока скритність - мітки «відкликають» тільки після опромінення спеціальним устаткуванням радіолокації імпульсом.

Подібні RFIDчіпи можна використовувати не тільки для оперативного стеження за людьми і автотранспортом, а й як превентивний захід по контролю за зброєю, наприклад вбудовувати їх в переносні зенітні ракетні комплекси або протитанкові ракети. У разі потрапляння цієї зброї в руки терористів його буде досить легко виявити і швидко знищити ракетним ударом.

Технологія тривимірного моделювання обличчя людини.

Всі описані вище технології мають один суттєвий недолік: потрібно підібратися до переслідуваного ближче. Однак це не завжди можливо.

Щоб від подібного «невидимого ока» сховатися було абсолютно неможливо, компанія PhotonX розробляє технологію тривимірного моделювання обличчя людини за кількома знімками з оптичних і інфрачервоних камер безпілотників. Спеціальне програмне забезпечення дозволяє створити детальний профіль голови людини за допомогою мультиспектральних датчиків і аналізу руху лицьових м'язів. Нова система дозволить ідентифікувати людину в натовпі і супроводжувати його без необхідності установки будь-яких маяків. Зрозуміло, оптичні сенсори не можуть стежити за людиною всередині будівлі, але зате вони можуть легко знайти його навіть на багато людній вулиці великого міста. Далі при необхідності ворога можна знищити ракетою або залучити агентів, які встановлять маяк. Система PhotonX вирішує головне завдання - спостереження за великою кількістю людей на великих просторах.

Можливості програми супутникового стеження за мобільними телефонами.

Сучасні GPS технологШІ можуть допомогти виконати пошук телефону, а також багатьох інших об'єктів через супутник. Здійснює все це супутникова система, що працює через спеціальну програму стеження (/ gps / programmaslezhenijazatelefonom).

Якщо система стеження використовується для спостереження за людьми, то у спостережуваного людини з собою завжди має бути спеціальний пристрій - персональний GPS-трекер або стільниковий телефон

фірм Nokia, iPhone, HTC з підтримкою функції GPS і операційною системою, наприклад, Android. Таким чином, цей мобільний телефон перетвориться на своєрідний «маячок» зі встановленою на ньому спеціальною програмою спостереження. Якщо використовувати програму стеження для спостереження за людьми, то мобільний телефон легко можна покласти в портфель або кишеню об'єкта, який потребує вашої контролі, або якщо необхідно GPSслеженіе за автомобілем, мобільний телефон можна покласти і в «бардачок». Після визначення програмою стеження точних координат, місцезнаходження та швидкості дані відправляються на сервер системи. Всі ці дані програма стеження отримує з заздалегідь заданою періодичністю.

Простежити за тим, як проводиться GPS-стеженння, можна в режимі онлайн: з комп'ютера або мобільного телефону. Крім місце знаходження об'єкта, що спостерігається в даний момент GPS-програма стеження дозволяє на електронній карті простежити напрямок руху і його швидкість. GPS система стеження зберігає всю історію пересувань відслідковуються об'єктів.

Сьогодні кожен бажаючий, озброївшись спеціальним програмним забезпеченням, має можливість простежити за діями будь-якого абонента стільникового зв'язку, тобто За допомогою спеціальних програм, таких як ShadowGuard, наприклад, можна прослухати переговори по чужому телефону або ж прочитати переписку по СМС.

Ще кілька років тому це було схоже на шпигунську фантастику, але сьогодні це реальність, і величезна кількість людей скористалося такою можливістю. А там, де є попит, як відомо із законів ринку, народжується і пропозиція. І на сьогоднішній день з'явилося безліч сервісів, які пропонують скористатися такою неймовірною можливістю.

Електронне антитерористичне спостереження.

Серйозний крок зробили і розвідувальні технології після подій 11 вересня 2001 року, коли були прийняті безпрецедентні заходи, навіть охарактеризовані в ЗМІ як кінець існування конфіденційної інформації в США. На особливу увагу заслуговує великомасштабний проект Міністерства оборони США

«Тотальна інформаційна обізнаність» (TIO). Він передбачає розробку і експлуатацію новітніх ІКТ, за допомогою яких можна здійснювати тотальне спостереження за рахунок масованого збільшення джерел інформації, перехоплення повідомлень будь-якого характеру, оперативного аналізу в режимі реального часу, тобто збору колосальної кількості даних, а головне - блискавичну реакцію спецслужб. Як стверджується, ці заходи будуть протидіяти терористичним загрозам за рахунок моніторингу місцезнаходження, пересувань і ділової активності населення, тобто Збору максимально широкої інформації про всі підозрілі явища, що вказують на плани терористів.

Система ТВО інтегрує всеосяжні цифрові дані про американських громадян, а також про іноземців, що мають контакти з населенням США, які слід поділити на два типи: особистісні (ділові, функціональні) і біометричні. Перші передбачається черпати з усіх існуючих баз даних як державного, так і

галузевого призначення: медичних, освітніх, торговельних, туристичних, телефонних, корпоративних, ветеринарних і т. д., А також з джерел, куди проникли все відстежуючі електронні пристрої: банківські рахунки, кредитні картки, оренда машин, транспортні агентства, медичні та ветеринарні записи, телефонні та інші комунікативні повідомлення, письмові, електронні, телефонні заяви громадян до держорганів і т.д. Біометричні дані - це зображення райдужної оболонки і сітківки очей, відбитки пальців, ДНК, графічні знімки особи і т. д.

Якщо врахувати, що при цьому використовується добре зарекомендувала себе традиційна техніка збору даних, наприклад просіювання телефонних рахунків, магазинних дисконтних карток і т. Д., Але вже через віртуальне сито, то збір інформації по лінії ТВО досягне безпрецедентних масштабів. Виникне унікальна централізована система, яка, подолавши роз'єднаність і недоліки численних наявних баз даних, буде містити точні дані, де знаходилася і що робила конкретна людина в заданий час. І тоді кожен громадянин США, будь то потенційний терорист або лояльний громадянин, виявиться під інформаційним ковпаком спецслужб.

Новий етап в епоху стеження за об'єктами пов'язаний з космічними літальними апаратами, зокрема супутниками, можливості яких безмежні. Причому передаючі супутники можуть рухатися по певній траєкторії, фіксуючи все на своєму шляху, а стаціонарні - предмети і їх пересування в одній географічній точці.

Супутники, оснащені спеціальними приладами, не тільки бачать, але і чують, відстежуючи різноманітні комунікативні процеси. Це своєрідні динамічні бази даних, вони не тільки збирають і зберігають інформацію, а й можуть відправляти її на Землю в заданому режимі. Наявність коду оберігає її від розшифровки.

Розпізнавання осіб злочинців і терористів на базі нейронних мереж.

Чому технології розпізнавання осіб будуть все більш затребувані в системах безпеки? Навіщо пам'ятати постійно зростаючу кількість паролів для різних сервісів і придумувати все болем складні способи ідентифікації себе в Інтернеті, коли у кожної людини з народження є унікальний ідентифікатор - його обличчя?

Найбільший онлайнторговец, китайська Alibaba Group, в 2015 р. оголосила про швидкий запуск системи Smile to Pay, яка дозволить покупцям входити на сайт і підтверджувати покупки, дивлячись в камеру смартфона. І це лише одна з безлічі перспективних напрямків технології розпізнавання осіб.

У питаннях розпізнавання осіб для забезпечення безпеки залізничного транспорту головним експертом може виступити Японія. Саме в цій країні в сферу рейкових перевезень людей і вантажів впроваджено максимальну кількість високотехнологічних рішень. І це при тому, що Японія вважається світовим лідером за обсягом пасажиропотоку, що проходить через вокзали (а вокзали тут нерідко об'єднують і наземний, і підземний транспорт). Однак метрополітен Країни висхідного сонця, зокрема Токіо, вивели в авангард

дуже сумні події. Система безпеки в столичній підземці кардинально оновилася після березня 1995 року, коли релігійні фанатики з секти «Аум Сінрікьо» розпорошили на двох станціях отруйний газ. Тепер токійський метро буквально напхане сучасними відеокамерами - на 290 станцій їх доводиться кілька тисяч! Встановлені камери і в багатьох вагонах швидкісних поїздів. Також є камери, які спеціалізуються на виокремлення предметів і людей, які не рухаються протягом довгого часу. Усі відеозаписи надходять в єдиний ситуативний центр, куди стікається також вся інформація від патрулюють метро поліцейських. Крім того, є і спеціальні стереовідеокамери, здатні «засікти» сторонній предмет або людини на шляхах і скомандувати поїзду зупинитися.

У 2012 р. «Хітачі Кокусай Електрик» представила систему з камерою прихованого спостереження, що дозволяє обробляти базу даних в 36 млн осіб за 1 секунду.

Відповідно до заяв «Хітачі» ця висока швидкість виявлення досягнута розпізнаванням осіб шляхом розпізнавання картинок на етапі запису камери спостереження і угруповання отриманих схожих осіб. Система об'єднує особи, які повертаються в рамках 30° і мають мінімальний розмір на зображенні 40 × 40 пікселів.

У 2014 р ФБР США оголосило про успішний запуск в експлуатацію системи розпізнавання нового покоління (NGI). Її метою є розширення можливостей відомства по ідентифікації громадян, і вона повинна замінити стару, яка базується виключно на відбитках пальців. З 2011 р. система працювала в експериментальному режимі.

Основною особливістю NGI є те, що вона отримує і обробляє біометричні дані автоматично. Система працює за рахунок інформації, одержуваної з камер відеоспостереження по всій країні. Вона виявляє унікальні риси обличчя тієї чи іншої людини і зберігає їх в базі даних. Потім при розслідуванні злочину вона зможе провести швидкий аналіз знімків і виявити зловмисників. Для ідентифікації людини досить виявити, наприклад, характерний шрам на його обличчі або татуювання на тілі.

ФБР розробило NGI спільно з Lockheed Martin, Security Solutions і IBM. Метою програми оголосили боротьбу з тероризмом і злочинністю завдяки поліпшенню способів біометричної ідентифікації, а також вироблення нових методів аналізу архівної інформації в результаті досліджень, оцінки і застосування перспективних технологій.

За допомогою цієї системи теоретично можна розпізнати людину з будь- якої фотографії, якщо інформація про нього міститься в базі даних. Подібні менш комплексні методи ідентифікації давно використовують такі компанії, як Facebook, їх технології дозволяють автоматично ідентифікувати того чи іншого користувача на завантаженій в соціальну мережу фотографії. Проект розробки NGI розрахований на 10 років, і в нього вкладено 1,2 млрд дол. США**.**

У 2011 р. система автоматичного розпізнавання осіб почала функціонувати в експериментальному режимі. Правоохоронні органи США

отримали від ФБР програмне забезпечення, яке дозволяло миттєво порівнювати фотографії підозрюваних з базою даних. Число американських відомств, що використовують її, стає дедалі більше. NGI дозволяє вести спостереження за людьми, які займають відповідальні посади. Наприклад, до них відносяться касири, вчителі, працівники соціальних служб, тобто Ті, кому необхідно здати відбитки пальців і фотографію при прийомі на роботу. Система дозволяє правоохоронним органам кожного штату протягом 24 годин дізнатися, чи не зробив чоловік, який претендує на таку посаду, який-небудь злочин. ФБР тільки попереджає місцеві правоохоронні органи про те, що здобувач уже був одного разу заарештований, а далі їм пропонується приймати рішення, що з ним робити, самостійно. Ця система допомагає також стежити за громадянами, звільненими з місць позбавлення волі достроково. Якщо колишній арештант вчинить злочин в одному штаті країни, то ця інформація дуже швидко буде доступна владі інших штатів.

Крім розпізнавання осіб NGI здатна ідентифікувати людину по його зіниці.

Системи ідентифікації нового покоління ведуть пошук осіб по базі з фотографіями понад 50 млн громадян. У штаті Нью-Йорк система розпізнавання осіб вже працює в Управлінні автотранспорту. Завдяки їй влада заарештувала понад 100 осіб і відкрили майже 1000 розслідувань.

У США в червні 2017р. почалися перші випробування системи розпізнавання осіб в кількох аеропортах. Пасажирам авіакомпанії JetBlue Airways, що стала ініціатором експерименту, не доведеться навіть діставати свої паспорти та інші документи, щоб потрапити на борт літака. Адже новій системі досить побіжно глянути на обличчя людей, щоб перевірити їх через бази даних служб безпеки і зареєструвати на рейс. Для того, щоб втілити цей проект в життя, JetBlue Airways об'єднала зусилля з Митною службою і Прикордонним патрулем США. За програмну сторону проекту відповідає компанія SITA.

Робота нової системи ґрунтується на звірці особи людини з зберігається в базі даних фотографією. Людям не потрібно буде пред'являти взагалі ніяких паперів або заздалегідь реєструватися, щоб взяти участь в цій програмі. У процесі розпізнавання людині всього лише потрібно встати навпроти камери, яка моментально сканує обличчя і звірить його з базою даних.

Подібні випробування в цій області проводять фінська авіакомпанія Finnair, голландська KLM, а також міжнародний аеропорт Париж -Шарль де Голль. У деяких випадках система розпізнавання осіб буде тільки дублювати дії співробітників служби безпеки, так як в даний момент вона не показує 100% - ного результату і іноді неточна.

На чемпіонаті світу з футболу 2014 року в Бразилії поліція була оснащена сонячними окулярами з прихованими камерами, які відстежували і ідентифікували по кримінальній базі до 400 пар очей в секунду на відстані до 12 миль (оптимізовані для роботи на відстані 50 м). Окуляри - прихована камера підключені по бездротовій мережі до бази даних, яка порівнює особи

з профілями 13 млн еталонів і сприймає 46 тис. Точок на обличчі для розпізнавання та ідентифікації збіги.

Окуляри - прихована камера можуть не тільки ідентифікувати злочинців, а й відображати поліцейському подальші вказівки до дії на заході.

Вчені Інституту Макса Планка в Саарбрюккені в Німеччині демонструють спосіб ідентифікації людини за кількома фотографіями, навіть якщо на більшості з них його обличчя закрите. Розроблена дослідниками система, яку вони називають «Безлика система розпізнавання», тренує нейронну мережу за допомогою безлічі фотографій, які містять як закриті від спостереження, так і абсолютно очевидно особи, а потім використовує ці знання, щоб ідентифікувати людину з закритим особам, шукаючи подібності в області голови і на інших ділянках тіла. Точність системи змінюється в залежності від того, скільки є фотографій в наборі з добре видимим зображенням обличчя. Навіть тоді, коли є тільки 1,25 копій зображень повністю видимого особи людини, система здатна ідентифікувати приховані від огляду особи з точністю 69,6%; якщо є 10 копій зображень добре відомого особи, точність збільшується до 91,5%.

В Швеції компанія Axis створила перший в світі «розумний» кодек (програмний перетворювач сигналу), створений для IPвідео і IPвідеоспостереження. Камера служить тільки першою ланкою, не тільки сприймає і транслює, а й інтелектуально обробляє зображення. Велика кількість охоронних агентств використовують технології аналітики як початковий рівень захисту, особливо вночі.

Китайська компанія Baidu, що займається створенням вебсервісів, на початку 2017 року успішно використовувала технологію штучного інтелекту для пошуку людини. Зникла дитина возз'єдналася з сім'єю через 27 років.

Компанія Baidu використовує базу з 200 млн зображень для того, щоб удосконалювати роботу системи розпізнавання осіб. Глава компанії Baidu Р. Лі вніс пропозицію про створення централізованої бази даних з відомостями про зниклих дітей, щоб допомогти возз'єднатися ще багатьом сім'ям.

Ще в 2010 р. в Росії створена перша повністю вітчизняна біометрична система моментального розпізнавання особистості в натовпі. Розроблено вона компаніє ю-інтегратором «Техносерв» і називається «КаскадПоток». Система нічим не поступається закордонним аналогам. Вона ідентифікує особу в режимі реального часу шляхом зіставлення відеоданих, отриманих, наприклад, з камер відеоспостереження, з зображеннями в базах даних оперативних обліків. На все це йде лише частка секунди, а ймовірність правильного розпізнавання досягає 94%.

У 2013 р. в петербурзькому метро на додаток до вже діючих камер, пунктів огляду і рамкам металлодетекторів впроваджена «інтелектуальна» система відеоспостереження. Базується вона на комплексі «КАРС» (комплексної автоматичної розшукової системі). Він заснований на системі

«Інтелект», розробленій ФСБ Росії для розшуку злочинців. Рішення складається з мережі відеокамер і серверів для обробки інформації. Спираючись на біометричні дані, система здатна автоматично розпізнавати

людей в натовпі і аналізувати їх схожість з особами, занесеними в базу даннях злочинців і підозрюваних. Якщо схожість перевищує 90%, система сповіщає про це поліцейських. Мало того, система навіть умент стежити за потенційним правопорушником за допомогою декількох камер.

У московському метрополітені вже створено єдиний інформаційний радіопростір, що дозволяє співробітникам підземки швидко зв'язуватися зі службою охорони, станції і потяги обладнані системою відеоспостереження, на платформах встановлені колони екстреного виклику. Планується оснастити кожну станцію додатковими камерами, а також турнікетами, здатними розпізнати вибухові пристрої, небезпечні предмети, отруйні та радіоактивні речовини.

Компанія NTechLab розробила сервіс FindFace для пошуку людей по фотографіях в «ВКонтакте». Сервіс пропонує 30 безкоштовних пошуків щомісяця, щоб використовувати його частіше і отримати додаткові настройки, потрібно купити платну підписку. Більшість звичайних користувачів познайомилися з технологією розпізнавання осіб саме завдяки FindFace.

Правоохоронні органи вже використовують технологію додатку FindFace, що дозволяє зв'язати фотографію людини, зроблену на вулиці, з його профілем в соціальних мережах, для пошуку злочинців і порушників.

У травні 2016 р. творець технології А. Кухаренко домовився з урядом Москви про тестування технології розпізнавання осіб на відео, які знімають міські камери. Їх в столиці дуже багато: 98 тис. на під'їздах, 20 тис. у дворах.

Якщо на людину показується високий ступінь подібності, то попередження про це відсилається співробітнику поліції, який знаходиться поруч. Алгоритм також зможе виділяти окремих людей в будь-якій частині міста і знаходити їх сторінки в соціальних мережах, з яких майже завжди можна дізнатися багато про їх життя, шукати учасників протестних мітингів. Навіть якщо людина забула телефон вдома, його переміщення по місту можна буде відстежити, якщо він потрапить в об'єктиви камер, і пов'язати з профілем в «ВКонтакте». У поліції використовують технологію для розкриття злочинів: беруть фотографії, проганяють через додаток, знаходять профілі людей, бачать, що вони вчора були онлайн, роблять запит у «ВКонтакте», там видають IP-адресу, звідки людина заходила.

Нейронна мережа дає набір ознак, за яким можна відрізнити одну людину від іншого (колір і форма очей, міміка та ін.).

Але більшість ознак, які видає нейронна мережа, не видимі людському оку. Точність зображення нейронною мережею складає близько 90%, а людиною - 25% (при обсязі бази, наприклад, 10 тис. Фотографій).

Алгоритм NTechLab дає можливість порівнювати пари осіб з 99% ступенем точності і проводити пошук по досить великій базі фотографій менш ніж за 0,3 секунди з точністю понад 70%. Ця технологія була визнана кращою на світовому чемпіонаті The MegaFace Challenge, організованому Університетом Вашингтона в 2015 р У цьому чемпіонаті взяли участь понад сто команд з усього світу, в тому числі і команда Google.

Для пошуку людини по базі з 1 млрд фотографій таким алгоритмом потрібно менше 1 секунди. Подібна швидкість пошуку може вирішити безліч завдань не тільки в масштабах міста, але і країни і навіть світу, наприклад, при пошуку злочинця в режимі реального часу. До переваг алгоритму крім швидкості пошуку по базах фотографій глобального масштабу відноситься дуже висока точність розпізнавання. Це стало можливим завдяки глибинному навчання і правильно підібраною архітектурі нейронної мережі.

Що чекає технології 3D розпізнавання осіб в Росії і в світі?

З поширенням автоматизації бізнес-процесів вони отримають все більш широке впровадження. Рівень якості технологій (точність розпізнавання зараз перевищує 95%) вже досить високий, а економія часу і ресурсів величезна. Трохи більше 10 років тому фотографії передбачуваних злочинців або банківських шахраїв порівнювали з наявною базою зображень вручну, і після 30й фотографії людина починає працювати повільніше і помилятися набагато частіше. Сьогодні все системи розпізнавання осіб не просто автоматизовані, а використовують штучні нейронні мережі. Це дозволяє їм працювати з колосальним об'ємом даних, покращать кількість помилок і збільшувати швидкість.

Компанія IDX і розробник - Центр мовних технологій в 2017 р. вивели на російський ринок сервіс віддаленої біометричної ідентифікації особистості - по обличчю і голосу. Партнери розраховують, зокрема, на прийняття законопроекту, який дозволяє такий спосіб ідентифікації для відкриття рахунків і видачі кредитів в банках. До 2019 року обсяг цього ринку в Росії може вирости до 325 млн дол. США.

IDX додала технології аутентифікації по обличчю і голосу від компанії

«Центр мовних технологій» (входить до групи Газпромбанку) в свою систему управління ідентифікацією. Таким чином, ці компанії зможуть ідентифікувати клієнтів не тільки з використанням документів, але і за допомогою біометричних даних. Для цього достатньо, щоб людина один раз створив і зберіг за допомогою спеціального додатку «цифрові зліпки» голоси і обличчя в інформаційній системі (що належить, наприклад, банку, оператору зв'язку, страхової компанії, авіакомпанії). За згодою клієнта такі біометричні дані можуть бути використані для віддаленого посвідчення особи всіма учасниками ринку без порушення цифрового суверенітету суб'єкта персональних даних.

Ідентифікація з використанням біометрії може зайняти болем 50% ринку ідентифікації протягом найближчих п'яти років в кредитних організаціях.

Проведення віддаленої ідентифікації - обов'язкова вимога

«антивідмивного» законодавства, зараз передбачає тільки два способи - через підтверджену обліковий запис клієнта на порталі держпослуг і підтверджується особливим способом набір персональних даних (паспортні дані і т. д.).

7. Використання дронів проти браконьєрів, терористів і

контрабандистів.

Одними з перших, хто почав використовувати безпілотники для охорони правопорядку, стали поліцейські США. Федеральне управління цивільної авіації (FAA), або вже понад 74 урядових агентств по використанню безпілотників в повітряному просторі країни, 17 з яких - правоохоронні.

Найбільш відомі серед них - Montgomery County в Техасі, Mesa County Sheriff's Department в Колорадо і Grand Forks з Північної Дакоти.

Дозвіл FAA дозволило силовикам абсолютно легально задіяти безпілотники для детального обстеження місць злочину і пошуку постраждалих людей. Однак американські поліцейські активно залучали вищевказані агентства до роботи і раніше, до отримання агентствами необхідних юридичних прав.

Поліцейські США намагаються використовувати дрони і в більш складних операціях, наприклад таких, як спостереження за потенційно небезпечними злочинцями.

Британські поліцейські почали використовувати практично безшумні Мультикоптер Black Hawk, що дозволяють вести відеозапис зі звуком.

Також стало відомо про плани британської поліції використовувати безпілотники в операціях з переслідування злочинців. За різними оцінками, це обійдеться силовикам набагато дешевше і безпечніше, ніж застосування мотоциклів, машин і вертольотів. Купівля дрона і його тривала експлуатація обійдуться в суму меншу, ніж одна погоня з використанням вертольота (що можливо далеко не завжди) і двох поліцейських машин. Крім того, застосування безпілотників ніяк не загрожує життю поліцейських.

Про перше успішне застосування квадрокоптера британською поліцією стало відомо ще в лютому 2010 року, коли за допомогою апарату AirRobot AR100B, оснащеного системою відеоспостереження і тепловізійної камерою, силовики графства Мерсісайд на заході Англії змогли розшукати в густому тумані автомобільного злодія. Подібні дрони застосовуються в Великобританії досі. Відомо, що технологія апарату спочатку розроблялася для потреб військової розвідки. Він практично безшумний і може працювати вночі, передаючи зображення в режимі реального часу.

З 2016 року робоча група при Раді керівників національної поліції і Центр прикладної науки і технологій обговорювали можливість використання БПЛА для переслідування підозрюваних, які використовують двох чотириколісні транспортні засоби для вчинення злочинів, говориться в заяві Служби столичної поліції Лондона.

Останнім часом лондонські поліцейські борються з ростом крадіжок, скоєних грабіжниками на мопедах і мотоциклах. За 12 місяців в британській столиці подібним чином було вкрадено болем 3 тис. Телефонів.

У той же час служба столичної поліції була змушена переглянути свою тактику переслідувань після інциденту, що призвів за собою загибель 18летній Г. Хікса. Молода людина загинула в гонитві на високій швидкості, намагаючись на мопеді піти від двох патрульних машин. Використання

дрона може знизити шанси повторення подібного інциденту.

У наприкінці 2015 р дрони надійшли на службу токійській поліції.

Вони увійшли в спеціальний загін по боротьбі з іншими дронами.

На даний момент безпілотники використовуються в правоохоронних органах цілого ряду країн. Однак варто зазначити, що поки поліцейські лише оцінюють потенційні можливості подібних апаратів. Так, в квітні минулого року мерія міста Дубай запустила в небо дрона-поліцейского, основним завданням якого стало стеження за екологічним порядком в місцях відпочинку і пустелі, а саме виявлення тих, хто кидає сміття мимо урн. Подібні дрони-поліцейські зможуть швидко з'являтися в різних місцях, знімаючи на камеру всіх порушників. При цьому особливо наголошується, що якщо дрони добре себе зарекомендують, силовики ОАЕ всерйоз задумаються про використання цих апаратів для більш складних завдань.

У Франції і Японії безпілотники активно використовуються для дистанційного спостереження за «скупченнями людей». Однак особливий інтерес викликають окремі підрозділи, які створюються в цих країнах з метою боротьби з випадками несанкціонованого використання дронів. Зокрема, поліція Токіо зовсім недавно заявила, що квадрокоптера, що порушують ті чи інші правила польотів, будуть відловлювати за допомогою спеціальних дронів БІЛЬШОГО розміру. Принцип роботи тут гранично простий: на превеликий квадрокоптера знизу прикріплюється мережу розміром приблизно 2 × 3 м. Далі такий апарат наздоганяє дрібні дрони-порушники і, піймавши їх мережею, виносить із забороненої зони.

Вперше на практиці подібний метод відлову дронів-порушників був випробуваний в лютому 2016 р. З цього моменту «дрони отлавліватели» справно несуть службу в лавах силовиків. Як сповіщає поліція Токіо, основна мета подібних робіт - захист важливих локацій «з урахуванням найгірших можливих сценаріїв», з чого можна зробити висновок, що мова тут, можливо, йде не стільки про знешкодження дронів папараці, які ведуть спостереження за приватним життям знаменитостей, скільки про протидії серйозній загрозі з боку дронів-терористів, озброєних вибухівкою. В сучасних умовах річ вельми актуальна, особливо якщо врахувати, що, за повідомленням Міністерства оборони РФ, вже відомі випадки використання безпілотників, начинених вибухівкою, в Сирії.

Також влітку 2016 р. ФСБ попереджала про плани терористів використовувати дрони для здійснення терактів в Європі.

Згідно з повідомленням ПРЕСЦЕНТР МВС в Росії безпілотники різних типів стали використовуватися поліцейськими починаючи з Олімпійських ігор 2014 року в Сочі. Дрони дозволяють співробітникам правопорядку ефективніше контролювати дорожню обстановку, проводити повітряну розвідку, боротися з браконьєрами і ін. Раніше стало відомо, що в червні 2016 р дрони дозволили співробітникам авіаційного загону МВС по Республіці Адигея за півроку виявити більше 150 порушень ПДР. А в Червоногвардійському і Майкопском районах безпілотники дозволили виявити порушення в сфері надрокористування і незаконні вирубки лісів.

Ізраїльська компанія Laser Detect Systems (LDS) представила на виставці HLS & Cyber Expo в ТельАвіве перший в світі безпілотник SpectroDrone, оснащений датчиками для визначення вибухівки і саморобних вибухових пристроїв з безпечної відстані.

Безпілотник використовує розроблену компанією лазерну систему виявлення вибухівки та інших небезпечних матеріалів в газах, рідинах, порошках з відстані в кілька кілометрів. SpectroDrone здатний виконувати ці завдання, маючи оперативний радіус дії в три кілометри.

Передбачається, що новий апарат можна застосовувати для розшуку баз і складів терористів, а також для виявлення мін і фугасів в зонах локальних конфліктів. В даний час для цих цілей використовують системи виявлення вибухівки, що розміщуються на автомобільній техніці, а також носяться комплекти і службових собак.

В країні крім безпілотників планується використовувати інфрачервоні камери для упіймання злочинців і визначення людей з холодною та вогнепальною зброєю.

Мер індонезійського міста Макасар заявив, що злочинців в місті будуть ловити дрони. Місто планує запустити дрони, які будуть переслідувати порушників під час погонь. Також апарати будуть оснащені системою розпізнавання осіб, щоб мати можливість визначати знаходяться в розшуку в натовпі. Макасар вже збирає різні біометричні дані своїх мешканців. Серед цих даних особи, відбитки пальців і скани райдужної оболонки ока. «У нас є біометричні дані всіх наших жителів - 1,8 млн осіб »,- сказав мер міста. Мер назвав громадську безпеку пріоритетним напрямком своєї діяльності. Крім дронів, розповів він, деякі вулиці обладнають інфрачервоними камерами, щоб визначити людей з холодною та вогнепальною зброєю. У місті 80% злочинів скоюють мотоциклісти, так що теплові камери спрямовані в першу чергу на них, так як визначити зброю в автомобілі їм не вдасться.

Перспективним для поліції є компактний квадрокоптер Snipe («Бекас») виробництва компанії Aero Vironment. Він проектувався як додаткове джерело інформації про супротивника для піхотинців армії США.

Основне призначення наноквадрокоптера - ведення візуальної розвідки на прилеглому ділянці місцевості. Snipe оснащений чотирма несучими гвинтами і важить всього 140 г. До моменту застосування дрон зберігається в невеликому легкому та міцному футлярі.

Перебуваючи в повітрі, Snipe виробляє відеозйомку за допомогою оптичної та інфрачервоної камер в режимі реального часу з високою роздільною здатністю, включаючи темну пору доби. Мобільність камер забезпечується вбудованим механізмом повороту. Отримана картинка відображається на блоці управління оператора.

На борту безпілотника знаходиться радіоапаратура - вбудоване УВЧ радіо і програмно обумовлена радіосистема SDR, що робить його доступним для широкого кола покупців.

Крихітний квадрокоптер, незважаючи на свої габарити, суверенно відчуває себе при поривах вітру до 24 км / ч, не створює зайвого шуму, що

дозволяє йому залишатися невидимим для супротивника навіть з близької відстані. У разі втрати радіозв'язку Snipe автоматично повертається до оператора.

Американський виробник нелетальної зброї Taser International заявив, що готовий надати поліції США безпілотники, оснащені електрошокерами. Компанія провела переговори з представниками поліції на конференції в СанДієго.

Влітку 2015 р. поліція США вперше в історії використовувала робота для нейтралізації злочинця. За допомогою робота Remotec F5, забезпеченого вибухівкою, поліцейські Далласа вбили М. К. Джонсона, який застрелив п'ятьох поліцейських під час вуличної акції.

«Після цього інциденту нам надходили питання, чи можливо обладнати зброєю Taser автономне транспортний засіб», - говорить представник Taser International С. Таттл. Тазер - електрошокові зброю несмертельної дії з радіусом дії до 10 м, що дозволяє проводити затримання правопорушника з мінімумом каліцтв.

У поліції США вважають, що застосування збройних тазером дронів може зберегти життя співробітників поліції під час небезпечних операцій, проте визнають, що це питання залишається дискусійним. «Неприйняття суспільством ідеї, що безпілотні літальні апарати можуть бути обладнані якимось видом зброї, - це перешкода, яке належить подолати», - говорить представник департаменту поліції Портленда П. Сімпсон.

У дослідницькій групі Police Foundation додали, що такі технології можуть бути ефективним засобом боротьби зі злочинністю, проте побоювання правозахисників з цього приводу вповні обгрунтовані. «Багато людей стурбовані тим, що якщо ви можете озброїти безпілотник електрошокером, то ніщо не завадить вам обладнати його вогнепальною зброєю», - каже президент організації Дж. Буерман.

У 2015 році влада штату Північна Дакота (США) прийняли закон, що дозволяє оснащувати дрони нелетальною зброєю. Поліція штату має право запускати безпілотники з електрошокерами, сльозогінним газом і травматичною зброєю.

Збройні дрони можуть стати по-справжньому грізною силою проти злочинців, і для цього в деяких країнах вже опрацьовується законодавча база. Наприклад, законодавчі органи Північної Дакоти ще в серпні 2015 р дозволила силовикам використовувати будь-яку зброю на безпілотники, крім вогнепальної. Іншими словами, поліцейські цього штату отримали можливість доповнити дрони стріляють електрошокерами, потужними розпилювачами газу і травматичною зброєю, що стріляє резиновими кулями.

На даний момент активно ведуться експерименти по оснащенню поліцейських дронів газовими балончиками. Більш того, французька компанія Drone Volt серійно випускає безпілотник TEAR GAS, який призначений для розпилення газу або перцевого екстракту. Однак про подібний практичному використанні дронів нічого невідомо - французькі силовики поки використовують ці апарати лише для дистанційного

спостереження за скупченнями людей.

Необхідно відзначити, що потенціал використання безпілотників в рядах правоохоронців може бути обмежений не стільки технічно, скільки юридично. Так, американський Союз захисту цивільних свобод ACLU вже висловив побоювання, що озброєння поліцейських безпілотників може стати причиною необгрунтованого застосування зброї, оскільки оператор дрона не присутній на місці подій особисто, а значить, не зможе адекватно орієнтуватися по обстановці. Також зараз активно ведуться дискусії з цивільними правозахисними організаціями з приводу законності використання дронів для спостереження за підозрюваними: чи є спостереження за потенційними злочинцями як втручання у приватне життя і чи є в подібних випадках какиелибо виключення?

8. Застосування роботів в профілактичній та оперативній роботі поліції.

Машини записують все, що відбувається навколо них (в 360°), на камери з високою роздільною здатністю - звичайні та інфрачервоні. При необхідності влаштування можуть використовувати мікрофон і динаміки для спілкування оператора з перехожими. Роботи зіставляють ряд предзапісанних параметрів, наприклад звуків, з потенційними злочинами - машини здатні реагувати на постріл, розбите скло і т. Д. Якщо підозрюється порушення, робот сохранітгеотег, зробить фотографії, передасть відеопотік. Пристрій збереже номера знаходяться поблизу автомобілів, обличчя перехожих.

У Кремнієвій долині для «охорони» кампусів і датацентрів були задіяні 24 пристрої. Глобальне завдання компанії - створити систему запобігання злочинів, засновану на роботах.

Стартапу вже вдалося зібрати близько 12 млн дол. США. Звичайно, про заміну охоронців супермаркетів або скорочення поліцейських мова не йде, однак пристрої можуть допомогти при розслідуванні низки злочинів і, можливо, запобігти вчиненню деяких з них.

Ще більш розумний патрульний робот створений в Китаї - Anbot. Його головна відмінність від каліфорнійського аналога в тому, що він не тільки помічає позаштатну ситуацію, але і легко може в неї втрутитися, по-перше, застосувавши електрошокові зброю (є підозра, що десь усередині робота також захований резервуар і для сльозогінного газу), по-друге , погнавшись за порушником (машина розганяється до 18 км / ч). Робот оцінює обстановку завдяки аудіодатчікам і камерам, розміщеним з усіх боків. Крім того, він здатний реагувати на нестямні крики жертв. Також в апарата є сенсорний екран, на якому можна натиснути кнопку SOS і попросити про екстрену допомогу. Робот важить всього 78 кг, зарядки акумулятора вистачає на 8 годин.

Також в Китаї (Пекін) в рамках міжнародної конференції 2015 г. «World Robot» відбулася презентація трьох бойових роботів китайського виробництва, призначених для боротьби з тероризмом.

Один з них виконує функцію хімікаразведчіка і сапера. В його обов'язки входить виявлення отруйних і вибухових речовин, після чого він негайно передає інформацію військовослужбовцям спецпідрозділів. Другий робот буде займатися утилізацією виявлених боєприпасів. Він важить всього близько 12 кг і може транспортуватися на спині бійця. Основне його призначення - допомога в індивідуальних місіях.

У разі виникнення «гарячих» ситуацій в справу вступить третій робот-боєць. Він оснащений зброєю невеликого калібру і гранатометом. У комплексі з сучасними прицілами робот зможе знищувати терористів на дальньої дистанції. Розробником є компанія з Харбіна HIT Robot Group. Серед потенційних покупців бойових роботів значиться пекінська поліція. Набір з трьох машин може обійтися в 1,5 млн юанів (235 тис. Дол. США).

На початку липня 2016 р поліцейського робота вперше використовували для вбивства злочинця: в Далласі був підірваний підозрюваний у стрільбі по поліцейським. Поліція зважилася на використання робота для вбивства злочинця, так як той відмовився вести переговори з правоохоронними органами. До гаражу, де переховувався стрілок, направили робота, який зазвичай використовується для знешкодження вибухових пристроїв. Робот не призначений для вбивства, але може переносити невелику кількість вибухівки, тому що при необхідності підриває великі підозрілі предмети. Цього разу до нього прикріпили приблизно 450 г пластичного вибухової речовини військового призначення С4. Цього вистачило, щоб при детонації на невеликій відстані від злочинця нанести йому травми, несумісні з життям. Сам робот практично не постраждав: пошкоджена тільки довга «рука», що переносить додатковий вантаж. За словами експерта в області військових технологій і автора книги «Змінюється характер війни» П. Сінгера, американці вперше використовували таку тактику всередині країни, але за кордоном американські роботи вже вбивали. В Іраку військові багато разів використовували в якості самостійного вибухового пристрою недорогого робота MARCbot (він коштує близько 15 тис. Дол. США). У Далласі вибух влаштував більш потужний робот Remotec Androx Mark V A1, який був придбаний поліцією в 2008 р за 151 тис.дол. США. Крім знешкодження бомб він може розбивати вікна, розпорошувати сльозоточивий газ, перерізати дроти, пиляти і пробляти отвори. Робот не самостійний, кожна дія контролює людина за пультом.

Крім Remotec Androx Mark V A1 в американській поліції «служить» і велика кількість інших роботів. Їх особливості проаналізував журналіст В. Воронін.

Найбільш популярні роботи, що підривають підозрілі предмети і деактивує вибухові пристрої; їх використання військовими помітно збільшилася під час воєн в Афганістані та Іраку.

Вартість подібних роботів коливається від 10 до 150 тис. Дол. США - в залежності від механізмів пошуку вибухових речовин і додаткових функцій. Як правило, поліція вибирає компактні моделі, щоб вони могли пролазити

під машини і проникати в різні приміщення. Часто роботи забезпечені мікрофонами і двома-чотирма камерами, які передають зображення в центр управління, а також потужними сенсорами, що визначають хімічний склад бомби. Поліція активно використовує модель PackBot 510 з детектором Fido, який «нюхає» бомбу і швидко визначає тип вибухівки. Від цього залежить вибір подальшої тактики - побилися або знешкодження на місці.

Іноді роботи допомагають поліції не ризикувати і діяти максимально акуратно при захопленні заручників. Прості моделі, забезпечені панорамними камерами і потужними мікрофонами, дозволяють оцінити кількість заручників і обстановку всередині будівлі, вести переговори із загарбниками, а також доставляти їжу і медикаменти на вимогу.

Для цих цілей використовуються навіть роботи, які зазвичай не працюють «кур'єрами». У квітні 2015 р апарат, знешкоджує бомби, передав телефон і піцу чоловікові, який планував вчинити самогубство і представляв загрозу для інших, тому-що тримав в руці ніж. Через годину після отримання піци і початку телефонної розмови з поліцейськими чоловік кинув ніж і здався.

Складні роботи-розвідники, наприклад BOZ 1, можуть розкривати двері, пробивати стіни і розбивати скла, щоб проникнути в закриті приміщення. Ще більш потужний робот Dragon Runner, розроблений компанією QinetiQ на замовлення Пентагону, вміє піднімати ся по сходах, рухати механічною рукою, фіксувати руху людей і підслуховувати їхні розмови на досить великій відстані. Одного разу в штаті Північна Кароліна цей робот пробрався до збройного чоловікові, який замкнувся в своєму будинку і не здався навіть після пуску сльозогінного газу. Перший апарат злочинець розбив на дрібні шматочки, але коли приїхав другий, між чоловіком і поліцією почалися переговори (через камеру і мікрофон у робота).

У деяких районах Кіншаси - столиці Демократичної Республіки Конго - автомобільним рухом керують людиноподібні роботи заввишки більше 2,5 м. Вони працюють як світлофори на перехрестях з особливо безладним рухом. Зелені, жовті і червоні вогні розміщуються на спині, грудях і руках роботів. На їх тулубах закріплені чотири камери спостереження, що фіксують порушення ПДР і оперативно відправляють дані в поліцейську дільницю. Кожен робот, виготовлений з алюмінію і живиться від сонячної батареї, коштує 21 тис. Євро.

Вже найближчим часом в експлуатацію потраплять відразу кілька роботів, які сильно змінять проведення поліцейських операцій.

Наприклад, в Німеччині в 2019 рік повинен з'явитися робот-сапер нового рівня. Передбачається, що співробітникам правоохоронних органів навіть не доведеться наближатися до підозрілих предметів, залишеним на вулиці: машина сама просканує речі і створить 3Dмодель закритою сумки. Робота аварійно-рятувальної служби зведеться до перегляду готових кадрів на комп'ютері: інженери повинні будуть проаналізувати отриману картинку, зробити висновки про те, чи є там бомба, і дати роботам наступні завдання в

залежності від ситуації.

У Дубаї в 2020 році повинні з'явитися самостійні роботи-поліцейські. Вони стежитимуть за безпекою на вулицях, в парках і торгових центрах. Правда, всі роботи будуть беззбройні, так що в екстреній ситуації не зможуть втрутитися, а тільки передадуть інформацію поліції. Роботи, наділені штучним інтелектом, повинні будуть також надавати довідкову інформацію на шести мовах, вміти жартувати і піклуватися про дітей.

Крім того, поліція Дубая запустила в 2017 р на вулиці міста автономну систему спостереження OR3, що складається з чотириколісних роботів і дронів. Систему спостереження розробила сінгапурська компанія Otsaw Digital. Колісний робот виглядає як маленький автомобіль. Він оснащений численними 3Di 2Dлазернимі сканерами, IMUсенсорамі і ультразвуковими датчиками, GPSнавігаторамі і передавачами даних на великі відстані. Завдяки системі уникнення перешкод він може безпечно пересуватися по дорогах і тротуарах. У задній частині робота вбудована висувна платформа, з якої відбувається запуск дрона, якщо необхідно встановити спостереження з повітря. Від наземного робота дрон може віддалятися на відстань 100 м. Система OR3 оснащена алгоритмами розпізнавання осіб і автомобілів (зокрема, номерних знаків), вона допоможе поліції Дубая шукати злочинців і «підозрілих осіб». Спочатку її будуть використовувати в туристичних районах Дубая.

У найближчі роки у поліції з'являться і спеціальні роботи для вбивства. В Ізраїлі в травні 2016 р представили модель, яка виглядає трохи крупніше ігрової приставки, але без проблем імітує з Вестн самозарядний пістолет Glock 26 на коліщатках.

І зовсім з області фантастики, яка фактично стала дійсністю, - кіборги. Дослідники з Університету Вашингтона в СентЛуісе перетворюють комах в кіборгів, яких можна відправити куди завгодно для винюхування вибухівки. Роботи ведуться на замовлення ВМС США. Дослідники вивчають, як комахи аналізують запахи. Виявлено, що сарана може ідентифікувати конкретні запахи, які їх навчили виявляти, навіть при наявності сторонніх запахів. Насекомиекіборгі будуть більш ефективними, ніж роботи, тому що вони використовують масу природних датчиків.

Навіть самі передові мініатюрні хімічні пристрої використовують лише кілька датчиків. Разом з тим, якщо подивитися на антену комах, то там кілька сотень тисяч датчиків різних типів. Для того, щоб перетворити звичайну сарану в машину попоіску вибухівки, інженери планують імплантувати в її мозок електроди, щоб підключитися до її антен у вигляді вусиків і розшифрувати електричні сигнали. Так як оператори повинні отримувати інформацію, зібрану комахами, дослідники також розробляють крихітний рюкзачок, який може передавати дані. На приймачі буде загорятися червоний світлодіод при наявності вибухових речовин, в той час як зелене світло сигналізує про відсутність загрози.

І, нарешті, інженери планують нанести татуювання на крила комах за допомогою біосумісного шовку, здатного перетворювати світло в тепло.

Лазер, який, ймовірно, буде в рюкзаку, по лить оператору контролювати дії кіборга. Фокусування лазера на лівому крилі забезпечить рух комахи вліво, і навпаки. Комаха буде функціонувати так само, як дістанціонноуправляемий дрон.

9. Нові технології прогнозування злочинної поведінки.

Вчені використовують чотири підходи до автоматичної класифікації об'єктів: метод опорних векторів; метод «k» (найближчих сусідів); логістичну регресію; використання згорткової нейронної мережі. Цим алгоритмам вони запропонували набір з тисячі вісімсот п'ятдесяти шести фотопортретів чоловіків (китайців віком від 18 до 55 років, без рослинності на обличчі, шрамів і татуювань, з нейтральним виразом обличчя), з яких 730 потрапляли під підозру поліції або мають кримінальний досвід (235 - у зв'язку з тяжкими злочинами). Ву і Джан окремо відзначають, що особи злочинців були показані на звичайних фотографіях, а не знімках, зроблених для поліцейських архівів.

Пройшовши навчання, всі чотири алгоритми продемонстрували певну здатність виділяти особи злочинців серед законослухняних громадян. Краще за інших показала себе згорткова нейронна мережа, точність прогнозів якої досягла майже 90%. Більш того, автори вказують на конкретні риси, нібито властиві кримінальній особистості, включаючи більш виражений вигин верхньої губи, менший кут між куточками рота і кінчиком носа, збільшена відстань між внутрішніми куточками очей.

Китайські вчені відзначають, що хоча комп'ютерний алгоритм дійсно «не обтяжений багажем суб'єктивності», від неї може страждати сама добірка осіб, на якій він навчався і перевірявся.

Дослідники могли, самі того не усвідомлюючи, відібрати особи, зручні для такої інтерпретації. Судді можуть виносити більш суворі рішення по відношенню до людей з більш суворими і жорстокими рисами обличчя.

Природно, робота китайських учених потребує більш серйозного обгрунтування і доопрацювання. Потрібно повторити експеримент з людьми різного віку, статі, етнічних груп і збільшити кількість наборів даних. Це повинно допомогти вирішити деякі спірні моменти. Наприклад, Ву і Чжан вважають, що кримінальні особи можна розділити на чотири підгрупи, а законослухняні тільки на три. Чому так відбувається? І як цей алгоритм буде працювати з іншими групами людей? У той же час дослідження вчених піднімає важливі питання. Якщо результат дійсно витримує критику, то як його пояснити? Чому у осіб злочинців набагато більше відхилень у порівнянні зі звичайними людьми? Як люди визначають злочинців? Це вроджене або придбане вміння? Якщо вченим вдасться відповісти на ці питання, тоді, можливо, робота вчених дасть новий виток розвитку антропометрії кримінального чи іншого характеру.

Крім того, влада Китаю зацікавились сферою предикативного аналізу, технології лицьового розпізнавання і іншими аспектами, пов'язаними з іноземними інвестиціями, які можна буде використовувати для запобігання

майбутніх злочинів. Аналізуючи моделі поведінки, влада буде повідомляти місцеву поліцію про потенційних злочинців.

Компанія Cloud Walk, офіс якої знаходиться в Гуанчжоу, проводить машинне навчання систем лицьового розпізнавання, а також аналізу і оцінки великих масивів даних для відстеження рівня ризику потенційних злочинців. Ті, хто є частими гостями магазинів з продажу зброї або часто відвідують різні транспортні вузли, найімовірніше, будуть відзначені системою. Під «підозру» можуть потрапити навіть відвідувачі господарських магазинів, тому як ці місця розглядаються владою зонами «підвищеного ризику»[1].

«Звичайно, якщо хтось купує кухонний ніж, то тут немає нічого кримінального. Але якщо ця ж людина навздогін купує мішок і молоток, то для системи він стане підозрілим », - зауважив представник компанії Cloud Walk в розмові з журналістом Financial Times.

Програмне забезпечення Cloud Walk вже пов'язано з мережі з базою даних поліції понад 50 міст і провінцій і може відзначати підозрілих осіб в режимі реального часу. В країні також вже діє система «особистісної переідентіфікацШІ», що використовується в якості запобіжного попередження злочинів: система здатна виробляти ідентифікацію людей в різних місцях, навіть якщо вони носять різний одяг.

«Ми можемо використовувати систему reID для пошуку підозрілих людей, які блукають туди-сюди в одній і тій же зоні або носять маски», - прокоментував виданню Financial Times Лінь Бяо, професор сфери образного розпізнавання в Пекінському університеті авіації і космонавтики.

Китай, безумовно, є одним з тих ідеальних місць, де подібні технології могли б використовуватися в повній мірі. Завдяки використанню більш 176 млн камер спостереження уряд має в своєму розпорядженні величезні вичерпні бази даних про своїх громадян. Іншими словами, країна надає величезний майданчик для збору всієї потрібної інформації і, отже, дозволяє ефективно навчати свої ШІсистеми, при цьому без яких-небудь юридичних перешкод.

Але це далеко не єдині шляхи, за допомогою яких Китай може розширити можливості своїх ШІсистем. Уряд цієї країни днями оголосив про масштабний, продуманий і профінансований план по перетворенню Китаю в світового лідера сфери ШІ до 2030 р.

Також ШІ може використовуватися для захисту особистого життя, інформації про здоров'я, фінансове становище, в якості засобу для запобігання хакерських атак. Штучний інтелект може відповідати за камери безпеки, роботів-охоронців і допомогти в створенні більш ефективних військових технологій; буде здатний як мінімум на 90% знизити кількість випадків автокатастроф.

Майбутніх злочинців можна виявити за будовою їх мозку в дитинстві. Розвиток і «здоров'я» мозку вже в трирічному віці може передбачити майбутній ризик опинитися в лікарні або в тюрмі. Про це повідомляється в статті, опублікованій журналом Nature Human Behaviour.

Працюючий в Університеті Дьюка (штат Північна Кароліна) нейрофізіолог А. Каспі і його співавтори проаналізували дані по більш ніж 1000 жителів Нової Зеландії, які народилися в 1972-1983 рр. і в трирічному віці проходили всебічне медичне, психологічне та соціальне обстеження. Вчені з'ясували і їх особисті історії аж до віку 38 років, в тому числі дані про приводах в поліцію і про звернення до лікарів.

Це дозволило виділити групу з 22% людей, які створюють максимальне «навантаження» на суспільство. Члени цієї невеликої групи відповідальні за 36% звернень до страховиків, 57% нічних відвідувань лікарень, 66% отримання державної допомоги, 77% залишених дітей, 78% виписаних ліків і 81% злочинів. Як зауважив Каспі і його колег, цей розподіл в цілому слід відомим принципом Парето, згідно з яким 20% зусиль дають 80% результату.

Вчені виявили, що потрапляння людини в цю групу можна з високою надійністю передбачити ще в трирічному віці за результатами обстеження розвитку нервової системи, мовних, моторних і пізнавальних навичок, а також особливостей характеру.

Кілька років тому Каспі і його співавтори запропонували узагальнювати результати таких тестів в єдиний р-фактор, індикатор нормального розвитку і стану мозку. І, хоча на становище людини в групі ризику впливають також соціоекономічні чинники, фактор «здоров'я мозку» (так його назвали автори статті) може служити хорошим провісником майбутньої долі.