

Міністерство внутрішніх справ України
Харківський національний університет внутрішніх справ
Кафедра іноземних мов факультету № 4
Науковий парк «Наука та безпека»

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВОПОРЯДКУ (зарубіжний досвід)

Збірник тез доповідей учасників
XXIII Міжнародної студентської
науково-практичної конференції
іноземними мовами,
присвяченої 30-річчю кафедри іноземних мов

12 квітня 2022 року, м. Харків, Україна

Харків 2022

*Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету
внутрішніх справ від 09.02.2022 № 16*

- Інноваційні** технології на службі правопорядку
174 (зарубіжний досвід) : зб. тез доп. учасників XXIII Міжнар.
студент. наук.-практ. конф. іноземними мовами, присвяч. 30-
річчю кафедри іноземних мов (12 квіт. 2021 р., м. Харків,
Україна) / МВС України, Харків. нац. ун-т внут. справ, Каф.
іноземних мов ф-ту № 4, Наук. парк «Наука та безпека». –
Харків : ХНУВС, 2022. – 248 с.

Збірник містить аналітичний огляд та узагальнення
зарубіжного досвіду використання інноваційних технологій
правоохоронними органами. Інформаційною основою
проведених досліджень є автентичні джерела англійською,
німецькою та французькою мовами. Матеріали конференції
сприятимуть удосконаленню та підвищенню ефективності
діяльності вітчизняних працівників поліції.

УДК 351.74:001.895](100)(06)

*Електронна копія збірника розміщується у відкритому доступі
на сайті Харківського національного університету внутрішніх справ
(<http://www.univd.edu.ua>) у розділі «Наука», сторінка «Конференції,
семінари та круглі столи», а також у репозитарії ХНУВС
(<http://dspace.univd.edu.ua/xmlui/>).*

ЗМІСТ

ПЕРЕДМОВА	16
------------------------	-----------

ТЕЗИ АНГЛІЙСЬКОЮ МОВОЮ

BEREZHETSKA A.	
INNOVATION TEHNLOGIE IN POLICE ACTIVITY	17
BIELIEVTSOV M.	
THE ETHICAL ISSUE OF POLICE USE OF QUADCOPTERS IN PRIVATE PROPERTY AREA	18
BLAGADYR I.	
A CRYPTOVIRAL EXTORTION TECHNIQUE: RANSOMWARE.....	19
BLUDOV K.	
LAW ENFORCEMENT ON THE FOREFRONT OF USING TECHNOLOGY TO IMPROVR PUBLIC SAFETY.....	21
BOHDANETS Ya.	
HOW ARTIFICIAL INTELLIGENCE IN POLICING HELPS CRIME DETECTION.....	22
BORSHCHOVA Ya.	
CYBERCRIME: OLD CRIMES IN NEW WAYS.....	23
BUKIR A.	
THREE LAYERS OF SKILLS NEEDED TO BE A LAWYER.....	24
BULYSH O.	
WAYS TECHNOLOGY BOOSTS CRIME-FIGHTING.....	25
CHAGOVETS D.	
TECHNOLOGICAL ADVANCEMENTS THATHELP SOLVE CRIMES	26
CHAIKIN T.	
INNOVATIVE TECHNOLOGIES IN THE SERVICE OF THE POLICE	28
CHAIKOVSKAYA D.	
UNINTENDED CONSEQUENCES OF TECHNOLOGY IN POLICING BY DR. JARROD SADULSKI	29
CHUBENKO R.	
ATTRACTING ROBOTS FROM BOSTON DYNAMICS FOR SERVE IN THE US POLICE.....	30
DATSENKO K.	
CRYPTOJACKING AS A MODERN CASH.....	32
DOBROZNAI N.	
UNMANNED AIRCRAFT SYSTEMS (UAS) USE IN POLICE WORK.....	33

DONCHENKO V.	
THE USE OF HIGH-SPEED RADARS ON THE ROADS OF UKRAINE	34
DULIN K.	
HANDHELD LASERS USE IN CRIME SCENE INVESTIGATION	34
FARTUSHNA D.	
NEW AND IMPROVED GADGETS HELP MINNEAPOLIS OFFICERS PREVENT CRIMES	35
GUTSAL V.	
THE FUTURE OF REGULATION	36
HORDUSENKO V.	
ISSUES WITH CREDIT CARD FRAUD DETECTION TECHNIQUES	37
HUNKO M.	
NONSTOP ADVANCEMENT ON LAW ENFORCEMENT TECHNOLOGY	39
KACHURIN B.	
THE FUTURE OF LAW ENFORCEMENT TECHNOLOGY	40
KALUGINA K.	
COMPONENTS OF CYBER SECURITY RISK MANAGEMENT SYSTEM	41
KALUZHNYAYA E.	
INNOVATION TECHNOLOGIES IN POLICE	42
KANAVCHENKO M.	
INNOVATIVE TECHNOLOGIES AT THE SERVICE OF LAW ENFORCEMENT AGENCIES	43
KANIUK A.	
NEW TECHNOLOGIES IN POLICE SPHERE	44
KHARA S.	
LIVE FACIAL RECOGNITION: EXPERIENCE OF UNITED KINGDOM	45
KHARCHENKO M.	
INNOVATIVE TECHNOLOGIES IN POLICE	46
KIRIIENKO V., ZAGORETSKA E.	
ECOLOGICAL CRIMINALITY IN UKRAINE AND FOREIGN COUNTRIES	48
KOBYLINSKA S.	
FIVE INNOVATIVE POLICE TECHNOLOGY IN ISRAEL	49
KORZH K.	
THE ADVANCEMENTS IN LEGAL TECHNOLOGY FOR THE CRIMINAL JUSTICE SYSTEM	51

KOSTENKO O.	
LABOUR EDUCATION AS AN EDUCATIONAL INNOVATION AIMED AT CREATING SAFE SOCIAL ENVIRONMENT	52
KOVAL D.	
DNA SAMPLES USE FOR CRIMINAL INVESTIGATION	53
KOVALENKO B.	
INNOVATION TECHNOLOGIES IN POLICING	54
KOVALENKO E.	
ROLE OF TEHNOLOGIES IN INDIAN CRIMINAL INVESTIGATION	55
KOZLIANSKA O.	
ADVANCEMENTS IN THE FIELD OF CRIMINAL JUSTICE	56
KRAVCHENKO Ya.	
COMPUTER FRAUD AND CYBER CRIME IN SOUTH FLORIDA	57
KULAK O.	
MOBILIZING TOOLS FOR FUTURE POLICING STRATEGY	58
KURILKIN O.	
CHANGING POLICE ECOSYSTEM FOR A SAFE FUTURE	59
KUSHCH M.	
USE OF THE LATEST FORENSIC TOOLS AND INNOVATIVE TECHNOLOGIES	60
KUZNICHENKO K.	
CLOSED CIRCUIT TELEVISION CAMERA AS A CRIME PREVENTION MEASURE	61
KYRYCHEKO D.	
INNOVATIVE TECHNOLOGIES FOR THE USE OF DRONS IN SWEDEN	62
MAKARENKO K.	
«DRONES AND ROBOTS IN UNIFORM: HOW TECHNOLOGY CHANGED THE POLICE»	63
MAKOVCHYK M.	
CHINA'S POLICE NEW WEAPON IN SURVEILLANCE	65
MALIARENKO D., SHUVALOV V.	
INNOVATIVE POLICE TECHNOLOGIES	65
MALYNOVSKA K.	
THE USA AND UK INTERNET AS AN AID TO CRIME PREVENTION	66
MINIAILO M.	
TECHNOLOGICAL INNOVATIONS IN POLICING AND CRIME PREVENTION	67

MIROSHNICHENKO A.	
VIRTUAL CONFERENCE TECHNOLOGY AS NEW SKILLS FROM LITIGATORS	68
MYTSYK L.	
HOW TOKYO POLICE USE DRONES.....	69
NAZARENKO D.	
PRE-CRIME TECHNOLOGY	70
NESKREBA T.	
BODY-WORN CAMERAS IN LAW ENFORCEMENT ACTIVITY	71
NEZHURINA Yu.	
THE FUTURE PERSPECTIVES OF POLICING.....	72
OBERNIKHIN O.	
THE USE OF ROBOTICS BY THE POLICE OF THE UNITED STATES	73
OSHCHEPKOVA A.	
INNOVATIVE TECHNOLOGIES IN THE SERVICE OF US LAW ENFORCEMENT.....	74
OSTAPENKO V.	
THE FACE RECOGNITION (FR) TECHNOLOGY. BIOMETRICS.....	75
PAVLENKO S.	
DRONES IN THE LAW ENFORCEMENT SERVICE.....	77
PIDGAINA V.	
INNOVATIVE TECHNOLOGIES	78
PILIPCHUK V.	
INNOVATIVE TECHNOLOGIES IN THE SERVICE OF LAW AND ORDER.....	79
POLTAVSKIY V.	
HOW BODY CAMERAS CAN HELP POLICE	80
PROKOPENKO R.	
SOME NEW POLICE TECHNOLOGY CURRENTLY IN USE	81
PRYKHIDKO D.	
LATEST TECHNOLOGIES FOR TERRORIST THREATS PREVENTIONS	82
REPALOV V.	
INNOVATION AND SCIENCE AS THE BASIS FOR IMPROVING LAW ENFORCEMENT.....	83
RIABTSEVA D.	
ROBOTS IN THE WORK OF LAW ENFORCEMENT AGENCIES.....	84
ROGOZHINA Yu.	
INNOVATIVE TECHNOLOGIES IN POLICE	84

ROMANOVA V.	
AN IMPORTANCE OF DATA COLLECTION AND INFORMATION GATHERING.....	87
ROSHENKO B.	
THE IMPORTANCE OF RELEVANT DATA COLLECTION FOR CRIME-FIGHTING.....	88
ROZUM A.	
HOW TO IMPROVE POLICE WORK THROUGH INNOVATION AND SCIENCE.....	89
SEMCHUK A.	
USE OF PROGRAMS FOR ANALYSIS OF NETWORK PROTOCOLS.....	90
SHEPELENKO R.	
INTELLETUAL PROPERTY THEFT AND HOW TO MANAGE YOUR IP TO STAY SAFE	91
SHEPILOVA T.	
THE MOST PERTINENT REASONS FOR THE RECENT SHIFT IN THE LEGAL INDUSTRY.....	92
SHEVCHENKO N.	
DATA PROTECTION IN THE SERVICE OF POLICE	93
STARCHENKO K.	
WILL POLICEMEN BE REPLACED BY ROBOTS?	94
SVISTUN D.	
INNOVATIVE TECHNOLOGIES IN THE POLICE.....	95
TALAN M.	
OPEN SOURCE INTELLIGENCE CRIME INVESTIGATION.....	97
TESLENKO O.	
PHISHING ATTACK AS A TYPE OF CIBERCRIME.....	99
TKACHENKO E.	
ADVANCED MODERN TECHNOLOGY HELPS POLICE FIGHT CRIME.....	100
TUYAHOVA Yu.	
OBSTACLES IN ORGANIZATIONAL COMMUNICATIONS	101
TYMOFIENKO I.	
INNOVATIVE TECHNOLOGIES IN POLICE	102
USENKO A.	
AUTOMATIC DEVICES IN THE SERVICE OF POLICE	103
USTYMENKO I.	
INNOVATIVE POLICE TECHNOLOGIES	104

VASYLCHENKO S.	
AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM USE IN POLICE WORK.....	105
VLASOV V.	
INNOVATIVE TECHNOLOGIES IN THE POLICE.....	106
YUDIN S.	
GUNSHOT DETECTION SYSTEMS USE IN US CITIES	107
ZADOROZHNA N.	
THE USE OF INNOVATIVE POLICE TECHNOLOGIES AS EXEMPLIFIED BY UKRAINIAN AND THE UNITED STATES POLICE.....	108
ZAHRUIKO O.	
A POLICE ROBOT AT THE CALIFORNIA LAW ENFORCEMENT SERVICE	109
ZHIZHIRIY O.	
HACKING: TYPES AND SECURITY.....	110
ZHURBA V.	
INNOVATIVE TECHNOLOGIES IN THE SERVICE OF LAW ENFORCEMENT IN CHINA	111
ZHYRONKIN D.	
TECHNOLOGY AND POLICE IN THE NETHERLANDS.....	112

ТЕЗИ НІМЕЦЬКОЮ МОВОЮ

BORYSIUK O.	
UAV FÜR ÖFFENTLICHE SICHERHEIT UND STRAFVERFOLGUNG	113
DAVYDOV O.	
DIGITALISIERUNG DER POLIZEIARBEIT	114
DOVBYSH A.	
MÖGLICHKEITEN DER KÜNSTLICHEN INTELLIGENZ IM STRAFVERFOLGUNGSSYSTEM	115
DZHYHA O.	
METHODEN DER 3D-TATORTDOKUMENTATION	116
KOVALENKO Ye.	
VIRTUAL REALITY IN DER VERKEHRSUNFALLPRÄVENTION	117
KULYK V.	
EINSATZ VON HUBSCHRAUBERN IM POLIZEIDIENST	118
NESHTA B.	
DIGITALE TRANSFORMATION IM BEREICH DER POLIZEITÄTIGKEIT	119

SKRYPNYK Ya.

IRISERKENNUNG ZUR IDENTIFIZIERUNG VON PERSONEN120

TELUKHA Ya.

INNOVATIVE TECHNOLOGIEN IN DER POLIZEI.....121

YANKOVSKA U.

VIRTUAL REALITY BEI DER POLIZEIAUSBILDUNG122

ТЕЗИ ФРАНЦУЗЬКОЮ МОВОЮ

MEDIANYK D. O.

LA ROBOTIQUE AU SERVICE DE LA POLICE123

SARVAEVA J. R.

MISE EN ŒUVRE DES MESURES OPÉRATIONNELLES
DE RECHERCHE DANS LE CYBERESPACE.....124

ТЕЗИ УКРАЇНСЬКОЮ МОВОЮ

БЕРЕЖЕЦЬКА А.

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ126

БЄЛЄВЦОВ М.

ЕТИЧНЕ ПИТАННЯ ВИКОРИСТАННЯ ПОЛІЦІЄЮ
КВАДКОПТЕРІВ У ЗОНІ ПРИВАТНОЇ ВЛАСНОСТІ127

БУКІР А.

ЩОБ БУТИ АДВОКАТОМ, ПОТРІБНІ ТРИ РІВНІ НАВИЧОК129

БЛАГАДИР І.

КРИПТОВІРУСНА ТЕХНІКА: ШКІДЛИВА ПРОГРАМА
З ВИМОГОЮ ВИКУПУ130

БЛУДОВ К.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ
ОРГАНІЗАЦІЯМИ ДЛЯ ПІДВИЩЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ ...131

БОГДАНЕЦЬ Я.

ЯК ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ
ДОПОМАГАЄ В РОЗКРИТТІ ЗЛОЧИНІВ133

БОРИСЮК О.

БПЛА ДЛЯ ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ
ТА ПРАВОПОРЯДКУ134

БОРЩОВА Я.

КІБЕРЗЛОЧИННІСТЬ: СТАРІ ЗЛОЧИНИ ПО-НОВОМУ135

БУЛИШ О.

ТЕХНОЛОГІЇ, ЯКІ ДОПОМОГАЮТЬ ПІДВИЩИТИ
БОРІТЬБУ ЗІ ЗЛОЧИННІСТЮ136

ВАСИЛЬЧЕНКО С. ВИКОРИСТАННЯ СИСТЕМИ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ТРАНСПОРТНИХ ЗАСОБІВ	138
ВЛАСОВ В. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	139
ГОРДУСЕНКО В. ШАХРАЙСТВО З КРЕДИТНИМИ КАРТКАМИ.....	140
ГУНЬКО М. БЕЗПЕРЕРВНИЙ РОЗВИТОК ТЕХНОЛОГІЙ ПРАВООХОРОННИХ ОРГАНІВ	142
ГУЦАЛ В. МАЙБУТНЄ ПРАВОВОГО ВРЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ	143
ДАВИДОВ О. ОЦІФРОВКА РОБОТИ ПОЛІЦІЇ	144
ДАЦЕНКО К. КРИПТОДЖЕКІНГ ЯК СУЧАСНА ГОТІВКА	145
ДЖИГА О. НОВІ МЕТОДИ ТРИВИМІРНОГО ДОКУМЕНТУВАННЯ МІСЦЯ ЗЛОЧИНУ	146
ДОБРОЗНАЙ Н. ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ (БПАС) У РОБОТІ ПОЛІЦІЇ	147
ДОВБИШ А. МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОННІЙ СИСТЕМІ	149
ДОНЧЕНКО В. ВИКОРИСТАННЯ ШВИДКІСНИХ РАДАРІВ НА ДОРОГАХ УКРАЇНИ	150
ДУЛІН К. ВИКОРИСТАННЯ ПОРТАТИВНИХ ЛАЗЕРІВ ДЛЯ ДОСЛІДЖЕННЯ МІСЦЯ СКОЄННЯ ЗЛОЧИНУ	150
ЖИЖИРІЙ О. ЗЛОМ: ВИДИ ТА БЕЗПЕКА	152
ЖИРОНКІН Д. ТЕХНОЛОГІЯ ТА ПОЛІЦІЯ В НІДЕРЛАНДАХ	153
ЖУРБА В. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ КИТАЮ.....	154

ЗАГОРЕЦЬКА Є., КІРІСНКО В. ЕКОЛОГІЧНА ЗЛОЧИННІСТЬ В УКРАЇНІ ТА ЗАРУБІЖНИХ КРАЇНАХ.....	155
ЗАГОРУЙКО О. РОБОТ-ПОЛІЦЕЙСЬКИЙ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ У КАЛІФОРНІЇ.....	157
ЗАДОРОЖНА Н. ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ПОЛІЦІЇ НА ПРИКЛАДІ УКРАЇНИ І США.....	158
КАЛУГІНА К. КОМПОНЕНТИ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ.....	159
КАЛЮЖНА Є. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	160
КАНАВЧЕНКО М. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ	161
КАНЮК А. НОВІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	163
КАЧУРІН Б. МАЙБУТНЄ ПРАВООХОРОННИХ ТЕХНОЛОГІЙ.....	163
КИРИЧЕНКО Д. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ДРОНІВ У ШВЕЦІЇ.....	165
КОБИЛІНСЬКА С. П'ЯТЬ ІННОВАЦІЙНИХ ПОЛІЦЕЙСЬКИХ ТЕХНОЛОГІЙ В ІЗРАЇЛІ.....	166
КОВАЛЕНКО Б. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	167
КОВАЛЕНКО Є. РОЛЬ ТЕХНОЛОГІЙ В ІНДІЙСЬКОМУ КРИМІНАЛЬНОМУ РОЗСЛІДУВАННІ	168
КОВАЛЕНКО Є. ВІРТУАЛЬНА РЕАЛЬНІСТЬ У ПРОФІЛАКТИЦІ ДТП	170
КОВАЛЬ Д. ВИКОРИСТАННЯ ЗРАЗКІВ ДНК ДЛЯ КРИМІНАЛЬНИХ РОЗСЛІДУВАНЬ	171
КОЗЛЯНСЬКА О. РОЗВИТОК ГАЛУЗІ КРИМІНАЛЬНОГО ПРАВА	172

КОРЖ К.

ДОСЛІДЖЕННЯ ЮРИДИЧНИХ ТЕХНОЛОГІЙ ДЛЯ СИСТЕМИ КРИМІНАЛЬНОЇ ЮСТИЦІЇ	173
--	-----

КОСТЕНКО О.

ТРУДОВА ОСВІТА ЯК ОСВІТНЯ ІННОВАЦІЯ, НАПРАВЛЕНА НА СТВОРЕННЯ БЕЗПЕЧНОГО СОЦІАЛЬНОГО СЕРЕДОВИЩА.....	174
--	-----

КРАВЧЕНКО Я.

КОМП'ЮТЕРНЕ ШАХРАЙСТВО ТА КІБЕРЗЛОЧИННІСТЬ У ПІВДЕННІЙ ФЛОРИДІ.....	175
--	-----

КУЗНІЧЕНКО К.

КАМЕРИ ВІДЕОСПОСТЕРЕЖЕННЯ ЯК СПОСІБ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ	177
--	-----

КУЛИК В.

ВИКОРИСТАННЯ ГЕЛІКОПТЕРІВ У ПОЛІЦЕЙСЬКІЙ СЛУЖБІ	179
---	-----

КУРІЛКІН О.

ЗМІНА ПОЛІЦЕЙСЬКОЇ ЕКОСИСТЕМИ ЗАРАДИ БЕЗПЕЧНОГО МАЙБУТЬОГО	180
---	-----

КУЩ М.

ВИКОРИСТАННЯ НОВІТНІХ КРИМІНАЛІСТИЧНИХ ЗАСОБІВ ТА ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ	181
--	-----

МАКАРЕНКО К.

ДРОНИ І РОБОТИ У ФОРМІ: ЯК ТЕХНОЛОГІЇ ЗМІНИЛИ ПОЛІЦІЮ	183
--	-----

МАКОВЧИК М.

НОВИЙ ЗАСІБ СПОСТЕРЕЖЕННЯ ПОЛІЦІЇ КИТАЮ	184
---	-----

МАЛИНОВСЬКА К.

ІНТЕРНЕТ США ТА ВЕЛИКОЇ БРИТАНІЇ ЯК ДОПОМОГА У БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ	185
---	-----

МАЛЯРЕНКО Д., ШУВАЛОВ В.

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В РОБОТІ ПОЛІЦІЇ	186
---	-----

МЕДЯНИК Д.

РОБОТОТЕХНІКА НА СЛУЖБІ В ПОЛІЦІЇ	187
---	-----

МИЦИК Л.

ЯК ПОЛІЦІЯ ТОКІО ВИКОРИСТОВУЄ ДРОНИ.....	189
--	-----

МІНЯЙЛО М.

ТЕХНОЛОГІЧНІ ІННОВАЦІЇ НА СЛУЖБІ ПОЛІЦІЇ ТА ПОПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ	190
---	-----

МІРОШНІЧЕНКО А.

ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ КОНФЕРЕНЦІЙ ЯК НОВІ НАВИЧКИ В СУДОВОМУ ПРОЦЕСІ	191
--	-----

НАЗАРЕНКО Д.	
АМЕРИКАНСЬКІ ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ.....	192
НЕЖУРІНА Ю.	
МАЙБУТНІ ПЕРСПЕКТИВИ ПОЛІЦІЇ	193
НЕСКРЕБА Т.	
НАГРУДНІ ВІДЕОРЕЄСТРАТОРИ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ	194
НЕШТА Б.	
ЦИФРОВА ТРАНСФОРМАЦІЯ У ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ	195
ОБЕРНІХІН О.	
ВИКОРИСТАННЯ РОБОТОТЕХНІКИ ПОЛІЦІЄЮ СПОЛУЧЕНИХ ШТАТІВ	196
ОСТАПЕНКО В.	
ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ОБЛИЧ (FR). БІОМЕТРИКА	197
ОЩЕПКОВА А.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ США	199
ПАВЛЕНКО С.	
ДРОНИ НА СЛУЖБІ ПРАВОПОРЯДКУ	201
ПИЛИПЧУК В.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВОПОРЯДКУ	202
ПІДГАЙНА В.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ	203
ПОЛТАВСЬКИЙ В.	
ЯК НАТІЛЬНІ КАМЕРИ МОЖУТЬ ДОПОМОГТИ ПОЛІЦІЇ	204
ПРИХІДЬКО Д.	
НОВІТНІ ТЕХНОЛОГІЇ ДЛЯ ПОПЕРЕДЖЕННЯ ТЕРОРИСТИЧНИХ ЗАГРОЗ.....	205
ПРОКОПЕНКО Р.	
ВИКОРИСТАННЯ НОВИХ ТЕХНОЛОГІЙ У ПОЛІЦІЇ	206
РЄПАЛОВ В.	
ІННОВАЦІЇ ТА НАУКА ЯК ОСНОВА ВДОСКОНАЛЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ	207
РОГОЖИНА Ю.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ У РОБОТІ ПОЛІЦЕЙСЬКИХ	208
РОЗУМ А.	
ЯК УДОСКОНАЛЮВАТИ РОБОТУ ПОЛІЦІЇ ЗА ДОПОМОГОЮ ІННОВАЦІЙ ТА НАУКИ.....	211
РОМАНОВА В.	
ВАЖЛИВІСТЬ ЗБОРУ ДАНИХ ТА ІНФОРМАЦІЇ	212

РОЩЕНКО Б.	
ВАЖЛИВІСТЬ ЗБОРУ ВІДПОВІДНИХ ДАНИХ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИНАМИ.....	213
РЯБЦЕВА Д.	
РОБОТИ В РОБОТІ ПРАВООХОРОННИХ ОРГАНІВ.....	214
САРВАСВА Ю.	
ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ У КІБЕРПРОСТОРІ	215
СВИСТУН Д.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	217
СЕМЧУК А.	
ВИКОРИСТАННЯ ПРОГРАМ ДЛЯ АНАЛІЗУ МЕРЕЖЕВИХ ПРОТОКОЛІВ	219
СКРИПНИК Я.	
РОЗПІЗНАВАННЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА З МЕТОЮ ІДЕНТИФІКАЦІЇ ЛЮДЕЙ	220
СТАРЧЕНКО К.	
ЧИ ЗАМІНЯТЬ РОБОТИ ПОЛІЦІАНТІВ?.....	221
ТАЛАН М.	
РОЗВІДКА З ВІДКРИТИХ ДЖЕРЕЛ	222
ТЕЛУХА Я.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В РОБОТІ ПОЛІЦІЇ.....	224
ТЕСЛЕНКО О.	
ФІШИНГОВА АТАКА ЯК ВИД КІБЕРЗЛОЧИНУ	225
ТИМОФІЄНКО І.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	226
ТКАЧЕНКО Е.	
НОВІТНІ ТЕХНОЛОГІЇ ДОПОМАГАЮТЬ ПОЛІЦІЇ БОРОТИСЯ ЗІ ЗЛОЧИННІСТЮ	228
ТУЯХОВА Ю.	
ПЕРЕШКОДИ В ОРГАНІЗАЦІЙНИХ КОМУНІКАЦІЯХ.....	229
УСЕНКО А.	
АВТОМАТИЧНІ ПРИСТРОЇ НА СЛУЖБІ ПОЛІЦІЇ	230
УСТИМЕНКО І.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	231
ФАРТУШНА Д.	
НОВІ ТА ВДОСКОНАЛЕНІ ГАДЖЕТИ ДОПОМАГАЮТЬ ПОЛІЦІЇ МІННЕАПОЛІСА ЗАПОБІГАТИ ЗЛОЧИНАМ	232

ХАРА С.	
РОЗПІЗНАВАННЯ ОБЛИЧ У РЕАЛЬНОМУ ЧАСІ: Д	
ОСВІД ВЕЛИКОЇ БРИТАНІЇ	233
ХАРЧЕНКО М.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ.....	234
ЧАГОВЕЦЬ Д.	
ТЕХНОЛОГІЧНІ ДОСЛІДЖЕННЯ, ЯКІ ДОПОМАГАЮТЬ	
РОЗКРИТИ ЗЛОЧИНИ	236
ЧАЙКІН Т.	
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПОЛІЦІЇ	238
ЧАЙКОВСЬКА Д.	
НЕПЕРЕДБАЧУВАНІ НАСЛІДКИ ВИКОРИСТАННЯ	
ТЕХНОЛОГІЙ У ПОЛІЦЕЙСЬКІЙ РОБОТІ:	
ДОСВІД ДОКТОРА ДЖАРРОДА САДУЛЬСЬКІ	239
ЧУБЕНКО Р.	
ЗАЛУЧЕННЯ РОБОТІВ ВІД КОМПАНІЇ	
«BOSTON DYNAMICS» ДЛЯ СЛУЖБИ В ПОЛІЦІЇ США	241
ШЕПЕЛЕНКО Р.	
КРАДІЖКА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ.....	242
ШЕПІЛОВА Т.	
НАЙБІЛЬШ АКТУАЛЬНІ АРГУМЕНТИ СУЧАСНОГО РУХУ	
В ЮРИДИЧНІЙ ГАЛУЗІ	243
ЮДІН С.	
ВИКОРИСТАННЯ СИСТЕМИ ВІЯВЛЕННЯ ПОСТРІЛІВ	
У МІСТАХ США	245
ЯНКОВСЬКА У.	
ВІРТУАЛЬНА РЕАЛЬНІСТЬ У НАВЧАННІ	
ПРАЦІВНИКІВ ПОЛІЦІЇ.....	246

ПЕРЕДМОВА

Це видання є збіркою тез XXIII Міжнародної студентської науково-практичної конференції іноземними мовами «Інноваційні технології на службі правопорядку (зарубіжний досвід)», присвяченої 30-річчю кафедри іноземних мов, яка відбулася у Харківському національному університеті внутрішніх справ 12 квітня 2022 року. У конференції взяли участь понад 100 курсантів і студентів України та зарубіжних країн.

У сучасному світі науково-технічні засоби, розроблені на основі новітніх досягнень природничих і технічних наук та впроваджені у практику правоохоронних органів, із кожним днем все більше і більше оптимізують їх діяльність. Сьогодні неможливо говорити про оптимальне забезпечення правопорядку без використання на практиці інноваційних технологій.

Інформаційний міжнародний обмін між ученими, працівниками правоохоронних органів та соціальними службами сприяє поширенню міжнародного досвіду на українську правову систему.

Учасники конференції розглядають широке коло питань у сфері використання інноваційних технологій органами правопорядку зарубіжних країн, чий досвід не лише стане в нагоді вітчизняним правоохоронцям, але й допоможе досягти передових позицій та сприятиме подальшому розвитку і підвищенню ефективності роботи поліції. Ключовими аспектами вивчення стали GPS-системи, системи мобільного зв'язку, робототехнічні системи, комп'ютерна техніка та новітні засоби спеціальної техніки.

Ретельне ознайомлення з матеріалами конференції свідчить, що, попри молодість і недостатній досвід авторів, ті підходи, які вони пропонують для вирішення окремих проблем, деякі висновки, до яких вони доходять, і пропозиції, які вони надають, безумовно заслуговують на увагу фахівців та подальше вивчення.

Слід зазначити, що за умовами проведення конференції надані матеріали додатково не редагувалися, тому відповідальність за їх зміст чи відповідність нормам тієї чи іншої мови несуть автори, їх наукові керівники та консультанти.

ТЕЗИ АНГЛІЙСЬКОЮ МОВОЮ

UDC 351.74:001.895](100)(06)

Alona BEREZHETSKA

Kharkiv National University of Internal Affair

INNOVATION TEHNLOGIE IN POLICE ACTIVITY

Policing technology has moved out of the backrooms of the administration building to the core of police operations.

Today police departments are using surveillance cameras, gunshot detection systems, automated license plate readers, facial recognition software, body cameras, drones, and numerous databases to prevent, respond and investigate crimes.

The near future holds even more possibilities, such as driverless patrol cars with heads-up screens, delivering information as the car patrols the streets. Augmented reality and artificial intelligence will eventually find its way into policing. Smart police uniforms could monitor and report on officers' stress levels and the surrounding environmental conditions and provide situational awareness to supervisors about their officers.

The question is not whether this technology exists, but rather, should police use it when it becomes available to them? And, if so, how should it be used?

We think these challenges can best be addressed by developing and using a digital ethics framework and a set of guiding principles that help create digital trust. Such a framework can help police leaders and their stakeholders think through the potential effects of technologies on officers and communities, identify unintended consequences and address the use of advanced technology for public safety.

Today, a successful business must understand the social and ethical consequences of using technology and work to mitigate negative consequences. Whereas this is arguably necessary for business, it is inescapably true for the public sector, particularly the police. Just as police leaders today work to build community trust, in the very near future they will have to be concerned with building digital trust.

Digital trust is created when an organization has good data integrity, security and control, and its use of technology and data is governed by a code of ethics. Digital trust between the police and their stakeholders could allow for a more rapid uptake of promising technology and mitigate some of the risks associated with it.

Digital ethics is broader and includes how technology and the data are used and the outcomes of that use. Transparent data and digital ethics create digital trust.

The following framework was developed by Accenture. Examples of the elements comprising data ethics and digital ethics are listed. It is a good place for police leaders to start thinking about digital trust.

As we move further into the 21st century, digital ethics and trust will become a primary issue for police. Your communities and your officers will demand the collection of data, the analysis produced, and use of the data, analysis and technology be secure and ethical.

Recent examples of how digital ethics and trust can play out are found in Chicago and New Orleans. Police departments in both cities found themselves explaining their use of algorithms to help create lists of high risk individuals. The two primary concerns emerging from these cities were around (1) transparency in what data was used and how the algorithm was generated, and (2) how the results were used.

Language adviser N. L Gorbach

UDC 351.74:001.895](100)(06)

Mykyta BIELIEVTSOV

Kharkiv National University of Internal Affairs

THE ETHICAL ISSUE OF POLICE USE OF QUADCOPTERS IN PRIVATE PROPERTY AREA

At the moment, with the development of unmanned operations, an ethical problem appears in filming materials, while flying in a private area. With the increased use of drones both by civilians and government agencies, it's essential for police department to craft effective law enforcement drone policy. Therefore, the need for legal regulation is not associated with the use of drones, but with the potential violation of the inviolability of personal property.

Drones, also known as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UAS), are aircraft that fly without a pilot on board.

Rules for the use of drones in Ukraine (for civilians) are :

Drones weighing up to 20 kg can be operated without receiving applications and permits for the use of airspace in compliance with the following rules:

- the maximum flight altitude is not higher than 120 m above the level of the earth (water) surface outside the established prohibitions and restrictions on the use of airspace;
- flights are not performed over crowded areas in open space and over densely built-up areas;

- the flight speed of the drone is no more than 160 km / h;
- flights are operated no closer than 5 km from the outer boundaries of the runways of aerodromes or no closer than 3 km from the outer boundaries of the runway / heliports;
- flights are operated no closer than 500 m from manned aircraft;
- flights are performed within line of sight (VLOS - visual line of sight);
- the drone does not cross the border of Ukraine.

In all other cases, a flight permit is required, with a precisely indicated route and flight objectives, which are issued by the State Aviation Administration of Ukraine.

Empowered to enforce the laws by which society has corporately agreed to be governed, police have a unique ethical attitude to the law. For an action to be ethical for police to take, it must first be legal. The law is a necessary deontological reference point for officers and agencies in defining right and wrong conduct. Unfortunately, in present conditions, legislation governing UAS use by police agencies is not enough. This circumstance creates a referential void for law enforcement executives seeking to put drone technology to use in service of the public. The absence of clearly defined ethical frames for drone use represents both a policy dilemma and a knowledge gap. The policy dilemma stems from the fact that the technology is out of the scope of regulation. These laws often vary greatly, which leads to inconsistencies from one jurisdiction to the other in such aspects as when drones may be flown in the nation's airspace. As the list of agencies seeking to use drones expands, the need for policy guidance and decision- making frameworks will grow.

Language adviser N. V. Krasnova

UDC [811.111:351.74(100)](06)

Inna BLAGADYR

Kharkiv National University of Internal Affairs

A CRYPTOVIRAL EXTORTION TECHNIQUE: RANSOMWARE

Ransomware is a type of malware from cryptovirology that threatens to publish the victim personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly

implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies that are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.

Ransomware malicious software was first confined to one or two countries in Eastern Europe and subsequently spread across the Atlantic to the United States and Canada. The number of cyberattacks during 2020 was double that of 2019. The first versions of this type of malware used various techniques to disable the computers by locking the victims system machine (Locker Ransomware). Ransomware uses different tactics to extort victims. One of the most common methods is locking the device screen by displaying a message from a branch of local law enforcement alleging that the victim must pay a fine for illegal activity. The ransomware may request a payment by sending an SMS message to a premium rate number. Some similar variants of the malware display pornographic image content and demanded payment for the removal of it. By 2011 ransomware tactics had evolved. Attackers began using electronic payment methods as well as language localization to the affected device. Corporations, private entities, governments, and hospitals can be affected by these malicious attacks. In 2016, a significant uptick in ransomware attacks on hospitals was noted. According to the 2017 Internet Security Threat Report from Symantec Corp, ransomware affected not only IT systems but also patient care, clinical operations, and billing. Online criminals may be motivated by the money available and sense of urgency within the healthcare system.

Factors that are key to a successful Cyber Awareness Training program is to establish a baseline identifying the level of knowledge of the organization to establish where the users are in their knowledge prior to training and after. Whichever approach an organization decides to implement, it is important that the organization has policies and procedures in place that provide training that is up to date, performed frequently and has the backing of the entire organization from the top down. Investment in technology to detect and stop these threats must be maintained, but along with that we need to remember and focus on our weakest link, which is the user.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Kiril BLUDOV

Kharkiv National University of Internal Affairs

LAW ENFORCEMENT ON THE FOREFRONT OF USING TECHNOLOGY TO IMPROVE PUBLIC SAFETY

As technology continues to make great developments, it is up to every state to ensure that their police officers are safe, honest, and efficient in the line of work that they do. Law enforcement agencies are on the right track by working with the Department of Justice to implement policies and programs that keep their officers safe and accountable. Aside from safety and accountability, more agencies need to work toward the implementation of control when it comes to body cameras. There isn't a need for technology to capture a phone call to the kids or even an officer using the restroom. As technology continues to evolve and make progressive changes, we're confident that implementing access and controls into body cameras can be done effectively to increase the pros and decrease the cons of technology in law enforcement.

We can just talk about the body cameras that modern police officers use. It should be noted that there are a number of other technologies that help in the work of the police. There some of them: Cloud computing.

As you know, information is key in policing. To do your job well, you need access to policies, procedures, and other crucial paperwork and documents. Cloud computing makes this possible. The PowerDMS platform 2017 State of Policy in Law Enforcement report revealed an increase in law enforcement agencies sending new policies and policy changes electronically using a cloud-based policy management software. This shift is in line with the increased demand from communities for accountability, and agencies are seeing it as a way to protect themselves and their reputation. Gone are the days of shuffling through file cabinets and thumbing through paperwork. The cloud allows police to both access and analyze data quickly and conveniently in several ways.

- Data collection and crime analysis.

Quickly tracking and analyze large amounts of data is important for law enforcement to do their jobs efficiently. Through cloud computing, police can access accurate statistics and real-time dashboards that monitor entire cities. They also have the ability to connect agencies to centralize criminal justice databases. This could lead to better information and decision-making.

- Document and records management.

Similarly, document management software can save officers a lot of time. When you house your policies and procedures in the cloud instead of in the office, they are accessible anytime, anywhere. This means your team can pull up crucial information when it matters most. Storing documents and records in the cloud can also save money on printing, paper, and filing supplies, so you can spend your resources on bettering your community.

- Online training.

Online training is another important tool in supporting officers. Having data and other documents readily accessible is one thing. But only when your team retains that information will they be successful. That's why training is crucial. Online training can supplement in-person, hands-on training, allowing officers to conveniently and quickly learn. This could save a lot of money and time, allowing your officers to be on the field as much as possible.

Police officers must receive the support, tools, training, and compensation they need and deserve so they can remain safe as they protect our communities.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Yana BOHDANETS

Kharkiv National University of Internal Affair

HOW ARTIFICIAL INTELLIGENCE IN POLICING HELPS CRIME DETECTION

Artificial Intelligence is slowly but surely becoming a proficient tool to punish the criminal and also to check unlawful actions. Many of the Law Enforcing Agencies across the world are using the most up-to-date solutions to prevent crime. Artificial intelligence in policing is a framework which is evaluated with the help of computers. It can also be utilized to make decisions regarding final rulings. It is the technology that holds great promise for the future in crime detection.

Thermal imaging has become an important police technology tool that is especially helpful in dark conditions. Thermal image cameras, some available as small hand-held units, utilize infrared imaging to detect heat emitted by such objects as humans and animals, and to deliver a "heat picture" or "heat map" of the environment in question.

It can be used to track the motion of suspects in a darkened building. Such technology has life-saving applications – from firefighting to search

and rescue missions (for example, finding a lost child or senior citizen in a blinding snowstorm).

The ongoing expansion of the Internet of Things (IoT) means more data is being generated, collected and analyzed than ever before – much of which can be incredibly valuable in a law enforcement context.

But the process of deriving actionable insights from immense amounts of data is so incredibly time-consuming that it is not remotely cost-effective when performed by humans. That's where artificial intelligence (AI) and its subcategory machine learning come in. AI is used to support many other police technologies, including ShotSpotter, facial recognition and biometrics.

Language adviser **L. S. Sazanova**

UDC [811.111:351.74(100)](06)

Yana BORSHCHOVA

Kharkiv National University of Internal Affairs

CYBERCRIME: OLD CRIMES IN NEW WAYS

What is Cybercrime? In Australia, the term cybercrime is used to describe both: crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks), and crimes where computers or ICTs are an integral part of an offence (such as online fraud)

Just as the internet and other new technologies are opening up tremendous possibilities, they also provide opportunities for criminals to commit new crimes and to carry out old crimes in new ways. On the evidence available, it is clear that the number, sophistication and impact of cybercrimes continues to grow and poses a serious and evolving threat to Australian individuals, businesses and governments.

Online, criminals can commit crimes across multiple borders in an instant and can target a large number of victims simultaneously. Tools that have many legitimate uses, like high speed internet, peer to peer file-sharing and sophisticated encryption methods, can also help criminals to carry out and conceal their activities.

The AFP is responsible for detecting, preventing, disrupting, responding to and enforcing cybercrime offences impacting the whole of the Australian economy. It focuses on investigating cybercrime threats against Commonwealth Government departments, critical infrastructure and information systems of national significance, with a key element being the

banking and financial sector. The AFP is guided by Commonwealth priorities for combatting cybercrime.

In general, the investigation of fraud against an individual is a state police responsibility. However, where there is a crossover between the investigation of a fraud against an individual and the investigation of an organised attack against critical banking systems, the AFP will work together with the local jurisdiction and the banking and finance industry. The AFP also works closely with State and Territory Police and international policing agencies in the fight against all types of cybercrime.

Nevertheless, ensuring you understand and practice good cyber security is the best way to combat cyber threats. The easiest way to stay on top is by turning on or confirming automatic updates where possible. An automatic update is a 'set and forget' feature that updates your software as soon as it becomes available.

Language adviser I. O. Gogol

UDC [811.111:351.74(100)](06)

Anastasia BUKIR

Kharkiv National University of Internal Affairs

THREE LAYERS OF SKILLS NEEDED TO BE A LAWYER

Law firms once viewed themselves as service providers, but about 20 years ago they began presenting themselves as experts with access to information that wasn't available to their clients. With the advent of the digital era, things have changed substantially and clients today expect a bit more. The current transformation, driven by technology, innovation, and collaboration, translates into the creation of valuable services. Nonetheless, law firms face a challenge: they must adopt a new mindset and acquire a new skill-set more akin to that of innovators who approach problem-solving from a different angle. Lawyers, like any other professionals, share a series of characteristic traits. Like leaders, lawyers are focused on problem-solving and have a strategic vision. The difference is that lawyers are combative, critical, rules-oriented and their default stance is adversarial. In contrast, leaders are creative, empathetic, collaborative and willing to take risks. Legal professionals must integrate the mindset of leaders and innovators into their way of working and providing services. Lawyers must be observant, develop relationships, and build networks, while constantly questioning everything in their search for solutions.

Legal service providers should have three layers of skills. Three layers of skills needed to be a lawyer:

The first layer consists of specific capacities related to three factors: the organization where the lawyers work or to which they provide their services; the services themselves; and technological factors. This layer includes skills related to project management, leadership, technology, sector-specific knowledge, business knowledge, marketing, communication, public speaking, and mentoring, among others.

The second layer includes what are called “collaborative” skills as well as skills related to creativity, which is essential to finding better solutions. Skills in this layer include empathy, inclusiveness, relationship-building, a growth mindset, multidisciplinary, diversity, and audacity – to name a few.

The third layer, consisting of client and service-focused skills, is where true innovation happens. These skills—which are the true source of leadership—are what set legal professionals apart from the rest.

When acquiring the skills needed to be a lawyer, most lawyers have traditionally focused on developing first-layer skills. Little effort has gone into the second layer, and the third layer has been neglected.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Olexander BULYSH

Kharkiv National University of Internal Affairs

WAYS TECHNOLOGY BOOSTS CRIME-FIGHTING

With reference to Pace University, technology helps law enforcement agencies and justice personnel stay one step ahead of criminals, furnishing new ways to detect and prevent crimes, as well as helping prosecutors convict offenders. And since emerging technology is available on both sides of justice, the cat-and-mouse game between perpetrators and police is never-ending, requiring continual adjustments from law enforcement agencies. The good news for public safety is that crime rates have generally decreased over the past two decades, due in part to advancements in crime detection and deterrent technology. Since effective policing leans heavily on the rapid sharing of sensitive crime-related data; the recent explosion in information technology is a positive development for law enforcement agencies. Identification technology, social media, and mobile capabilities also enhance public safety, enabling justice staff to do their business more efficiently and respond to unfolding investigations in real-time.

While technology poses challenges for law enforcement agencies, which continually strive to keep up with technology-based criminal enterprises; it does more good than harm in the fight against crime. Tech

advancements in law enforcement include the following capabilities, which illustrate how quickly things change alongside technology.

Sharing Information - law enforcement agencies are spread throughout a national criminal justice system that involves, regional, state, and local authorities, each administering their policing efforts independently. Sharing information about offenders also has a positive preventative impact, helping keep guns out of the hand of dangerous criminals and barring offenders from certain types of employment.

Security and Surveillance Upgrades - property crimes continue to decrease statistically, so security and video surveillance upgrades have improved public safety dramatically.

Social Media - though it is a social trend as much as it is a technological breakthrough, social media use nonetheless furnishes law enforcement advantages for agencies that use the technology effectively.

Crime Mapping Technology - modern computing power speeds up data analysis and enables law enforcement to track crime trends geographically.

Mobile Technology - mobile technology furnishes an electronic trail of texts, emails, calls and GPS location information that law enforcement uses to solve cases. Smartphones are so widespread the contact information and other data they contain give officers a starting point for their investigations, which often unfold in arrests directly related to information gleaned from mobile devices and usage.

Technology will never replace solid investigative work, but modern advances assist law enforcement efforts to stay ahead of criminals. Mobile technology, social media, and rapid access to information contribute to better enforcement and prevention. And crime-mapping and video surveillance breakthroughs also increase public safety, enabling justice agencies to direct resources to where they are needed most.

Language adviser I. O. Gogol

UDC [811.111:351.74(100)](06)

Diana CHAGOVETS

Kharkiv National University of Internal Affairs

TECHNOLOGICAL ADVANCEMENTS THAT HELP SOLVE CRIMES

Advancements in the last years have provided law enforcement professionals with technologies that not only make their jobs easier but also keep them safe at the same time. While this list could be endless, here are

some of the most important technological advancements that have aided in the battle against crime.

Data Mapping. The trend of data mapping isn't new; in fact, weather and climate scientists have been doing it for decades. However, criminal justice professionals are also data mapping now, providing police departments as well as federal agencies with a clear geographical look at the types of crime and the volume of crime that happens in an area. This is beneficial to law enforcement because it shows trends that may be able to be traced back to certain locations; drug rings are a prime example of how data mapping can be useful to the police. It also helps the police pinpoint problems in a community and allows them to strategize effectively to help reduce crime.

Smartphone Tracking. While there is some debate about when and how smartphone tracking should be utilized by law enforcement, the ability to track a criminal through the use of their smartphone is an incredible advancement in technology. This technology, when accessed through legal channels, can provide law enforcement with a clear picture of a suspect's movements before, during, and after a crime. For those innocent of the crime they are accused of, the technology can save them from a criminal trial; for those who are guilty, the tracking capability of this common object can seal their fate.

Social Media. Social media has had a large impact on law enforcement. Many law enforcement agencies and police departments have dedicated social media accounts on various platforms, enabling them to engage with their communities and act on tips in real time. This has become invaluable for solving crimes because it enables the police or other law enforcement to get up-to-the-minute information on an ongoing crime or a recent crime simply by paying attention to their social media feeds. It is also useful for gauging how a community feels about their interactions with the police; it is now clear that having direct engagement with law enforcement builds trust, enabling victims and witnesses to come forward with information on crimes.

Biometrics. Most Americans are used to biometrics; it is the technology that enables them to unlock their smartphones with a fingerprint or an iris scan. This technology has been around for decades but only recently has it become accessible to the public. The criminal justice field has now taken that technology and created smaller identification devices that make it possible to spot criminals with past records or outstanding warrants without having to wait for a process that could take weeks or months. These handheld devices can be used at a crime scene to collect digital fingerprints and then used on witnesses to see if a perpetrator is still at the scene of a crime.

Technology continues to improve law enforcement and, in turn, the relationship between law enforcement officers and the communities they serve. By providing various ways of dealing with crime, technology has made communities safer places to live and work in. With more advancements on the horizon, professionals who are seeking a criminal justice degree will find that technology will continue to play a large role in how the criminal justice field will look in the years to come.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Timofii CHAIKIN

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN THE SERVICE OF THE POLICE

In the US more than 910 organizations, including police and fire departments, use drones to help collect evidence and track events from a distance. According to former Philadelphia Police Deputy Commissioner Nola Joyce, law enforcement also uses gunshot detection systems, automatic license plate readers and facial recognition programs. Meanwhile, in the US, a mechanical engineer at the California-based research institute SRI International has designed a robot to help police officers avoid potential conflicts with motorists.

Another assistant system will soon appear with the police in the UK. With the help of it, law enforcement officers plan to predict the commission of serious crimes of a violent nature using artificial intelligence technologies. A combination of AI (artificial intelligence) and statistics is used. To search for "future" criminals, the system evaluates more than 1.4 thousand characteristics. AI algorithms calculate a person at risk and give an estimate of the likelihood of him committing a crime with the use of a weapon. About the use of digital technologies to improve the safety of employees and citizens: The Internet of Things and distributed sensing is the use of new technologies to collect information about the world and point in the right direction. But what should officers do at the scene? New technologies and methods are being developed that can help guide action in the world. Such advances in areas as 5G communications, miniaturization of electronics and augmented reality are enabling people to see, hear and act in ways that were previously impossible. For example, an officer arriving in an unfamiliar situation can now use augmented reality goggles to see relevant information about previous service calls from that address, find

building exits, or view the blocks recent crime history. With this information, the officer can take precautions to protect himself and serve the community

Language adviser **L. I. Rusanova**

UDC [811.111:351.74(100)](06)

Daria CHAIKOVSKAYA

Kharkiv National University of Internal Affairs

UNINTENDED CONSEQUENCES OF TECHNOLOGY IN POLICING BY DR. JARROD SADULSKI

Dr. Jarrod Sadulski is an adjunct professor with American Military University. He has spent more than two years studying police stress and its influence on the lives of police officers. He says: “While technology has undoubtedly been beneficial for policing, many of these advancements have also had adverse—and often overlooked—impacts on policing.”

Technological advancements have caused major changes in policing in the past several decades. Compared to past generations, officers today are surrounded by technology that is intended to increase productivity, officer safety, and agency efficiency. Communication, for example, has been dramatically improved. The days of communicating with dispatch only through the traditional police radio or tracking down a pay phone to call the station are long gone. Today, officers have cell phones and are responsible for monitoring communications through advanced police radios that can scan many channels or districts at one time. Police vehicles are also equipped with advanced computer-aided dispatch systems. These dispatch systems improve how quickly officers respond to calls for service, assist in the collection of investigative data, and clear calls without radio communication. There have been many other advancements as well. For example, conducted energy devices such as Tasers have been deployed in more than 7,000 police agencies. Research shows that these devices have contributed to a reduction in officer injuries by 25 to 62 percent (MacDonald, Kaminski, & Smith, Michael 2009). Other technologies have also helped officers be more efficient and effective. For example, traffic-light cameras have enabled patrol officers to focus on problematic areas and assisted them with traffic enforcement.

There is an inherent amount of stress involved with learning and applying many of these advanced technologies. Officers are expected to embrace technology and, unfortunately, do not always receive the proper training needed to use it at a mastery level. Many officers feel that different technologies are pushed on them, creating an unmanageable number of

things to learn and remember. It is important for agency leaders to realize that adapting new technology often causes stress for officers so they need to take steps to help alleviate some of that stress. Technology can have unintended consequences when officers must pay attention to so many different devices. For example, even though computer-aided dispatch systems, cell phones, and other communication devices each have their benefits, they can be extremely distracting for officers and even dangerous when their full attention is needed on a single situation. For example, while an officer is driving a patrol unit, calls for service are typically pushed to the officer's in-vehicle laptop through the computer-aided dispatch system. Referring to this technology while driving puts officers at an increased risk for vehicle accidents. Having to constantly divide their attention between different devices can result in a potentially dangerous situation and cause officers ongoing stress. Another source of stress for officers is that some of these technological advancements won't work when they need it. Officers are now equipped with less-than-lethal advanced weapons like Tasers and ammunition that includes pepper rounds, and rubber projectiles. If these devices don't work as expected, officers may be hurt.

At a time where stress management in policing is critical to promote resiliency and good health in officers, steps can be taken to reduce the stress that is associated with technology. Examples include: enacting administrative policies or personal goals designed to reduce distractions; set a standard for communication with dispatch and supervisors while on duty; permit officers to use the technology they're comfortable with, when possible; Provide proper time for training officers on new technologies.

In conclusion, technology has resulted in many advantages for law enforcement. Advanced technological equipment can reduce manpower shortages, increase officer safety, and help officers do their job more easily. However, technology can also become a stressor for officers. It is important that agencies recognize this stress and take steps to help officers become proficient and comfortable using technology

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Ruslan CHUBENKO

Kharkiv National University of Internal Affairs

ATTRACTING ROBOTS FROM BOSTON DYNAMICS FOR SERVIE IN THE US POLICE

Boston dynamics is a leading American engineering company that has been producing dog robots and other robotics since 1992. In 2019, the Massachusetts Police Department became the first law enforcement agency

in the United States to use a Boston Dynamics robot called Spot. According to Wbur News Spot, as well as other work of the department, used as a "mobile remote surveillance device" to provide military personnel with images of suspicious devices or potentially dangerous places, such as where an armed suspect may be hiding.

"Robot technology is a valuable tool for law enforcement because it can inform about potentially dangerous environments," wrote David Procopio, a state police spokesman. The peculiarity of Spot is that it is a dog-like robot that works without recharging for an hour and a half, moves at speeds up to 5.8 km / h, and has a load capacity of up to 14 kg and can withstand temperatures from -20 ° C to 45 °C. It also has a 360-degree low-light camera and an arm.

In 2021, the "robocop" was used in two operations. In the first case, there was an operation to rescue hostages, then criminals took people against their will and kept in one of the apartments. Spot, equipped with a camera and lanterns, was launched into the room, as a result, all went without casualties, and the perpetrators simply fled.

The second case of use was when the criminal was detained, the robopese was used as an observer.

Another difference between Boston Dynamics and their Spot creation from other police robotics companies is that the company-police agreement precludes the use of the robot as a weapon, so it is rented out, not sold. According to Michael Perry, vice president of business development at Boston Dynamics, this was done so that the company could withdraw from work if it finds a breach of contract.

According to DW after the successful use of Spot robots from Boston Dynamics in the US, the Netherlands was the first in Europe to buy a robot to perform their task of being spies in drug labs, to protect special forces personnel and ordinary citizens from armed attack or defeat toxic substances.

To do this, Spot is equipped with special sensors and video cameras that transmit all information in real time to the operator's screen.

Thus, summing up, we can say that the involvement of innovative technologies in policing not only increases the efficiency of the police, but also increases the level of protection of the population and personnel.

Language adviser N. V. Krasnova

UDC [811.111:351.74(100)](06)

Kateryna DATSENKO

Kharkiv National University of Internal Affairs

CRYPTOJACKING AS A MODERN CASH

Cryptojacking is a type of cybercrime where a criminal secretly uses a victim computing power to generate cryptocurrency. Primary effects of cryptojacking include: device slowdown; overheating batteries; increased energy consumption; devices becoming unusable; and reduction in productivity. Cryptojacking in the cloud could also cause additional costs for businesses that are billed based on CPU usage..

Cryptojacking (also called malicious cryptomining) is an online threat that hides on a computer or mobile device and uses the machine's resources to "mine" forms of online currency known as cryptocurrencies. Malicious cryptominers often come through web browser downloads or rogue mobile apps. Cryptojacking can compromise all kinds of devices, including desktops, laptops, smartphones, and even network servers. Like most other malicious attacks on the computing public, the motive is profit, but unlike many threats, it's designed to stay completely hidden from the user. To understand the mechanics of the threat and how to protect yourself against it, let's begin with a bit of background.

Cryptocurrencies are forms of digital money that exist only in the online world, with no actual physical form. They were created as an alternative to traditional money, and gained popularity for their forward-looking design, growth potential, and anonymity. One of the earliest, most successful forms of cryptocurrency, Bitcoin, came out in 2009, and gained mainstream recognition in the years following. Bitcoin's success inspired dozens of other cryptocurrencies that operate in more or less the same way. You may be familiar with names like Ethereum or Dogecoin, for instance. Today, people all over the world use cryptocurrencies to buy things, sell things, and make investments. Two words—"cryptography" and "currency"—combine to form "cryptocurrency," which is electronic money, based on the principles of complex mathematical encryption. All cryptocurrencies exist as encrypted decentralized monetary units, freely transferable between network participants. Or put more simply, cryptocurrency is electricity converted into lines of code, which have a real monetary value.

Whether you've been cryptojacked locally on your system, or through the browser, it can be difficult to manually detect the intrusion after the fact. Likewise, finding the origin of the high CPU usage can be difficult. Processes might be hiding themselves or masking as something legitimate

in order to hinder you from stopping the abuse. As a bonus to the cryptojackers, when your computer is running at maximum capacity, it will run ultra slow, and therefore be harder to troubleshoot. As with all other malware precautions, it's much better to install security before you become a victim.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Nazar DOBROZNAI

Kharkiv National University of Internal Affairs

UNMANNED AIRCRAFT SYSTEMS (UAS) USE IN POLICE WORK

If you thought remote control camera robots were cool, you will be excited to hear that some law enforcement agencies have experimented with using unmanned aircraft systems (UAS), sometimes known as drones. The UAS could be used to search for suspects, obtain information and survey disaster areas without using a piloted helicopter or plane. Not only could UAS technology save money, but it also has the potential to keep law enforcement officers out of harm's way.

The number of drones is constantly growing and air traffic authorities urgently need solutions to manage their presence in the airspace, the same as any other type of aircraft. Considering the specific characteristics of UAS operations, they should be as safe as those in manned aviation. Technologies for unmanned aircraft allow a wide range of possible operations. Requirements related to the airworthiness, the organization as well as the persons involved in the operation of UAS and unmanned aircraft operations should be set out in order to ensure safety for people on the ground and other airspace users during the operations of unmanned aircraft. The rules and procedures applicable to UAS operations should be proportionate to the nature and risk of the operation or activity and adapted to the operational characteristics of the unmanned aircraft concerned and the characteristics of the area of operations, such as the population density, surface characteristics, and the presence of buildings. The risk level criteria as well as other criteria should be used to establish three categories of operations: the 'open', 'specific' and 'certified' categories.

While this technology in law enforcement is currently available, the widespread use of unmanned aircrafts has been slow to take off due to regulations and critique from members of the public. Only time will tell if these unmanned aircraft will become a widespread part of our law enforcement.

Language adviser A. E. Korshenko

UDC 351.74:001.895](100)(06)

Vitalii DONCHENKO

Kharkiv National University of Internal Affairs

THE USE OF HIGH-SPEED RADARS ON THE ROADS OF UKRAINE

Recently the number of road accidents increased in Ukraine, due to the excessive speeding. Taking this fact into account, the National Police of Ukraine decided to counteract these crimes using high-speed Trucam radars on roads, which are widely used by police in Germany.

In Germany, violations are recorded by 3500 stationary radars, which are installed both on the highways and in the localities. Drivers are notified about the control and supervision by scoreboard with the inscriptions “Radarcontrol”.

In Ukraine, the number of areas in which the speed limit is measured with the Trucam device, has recently increased to 309. From Monday, March 22, 2021, patrol officers with the Trucam device began their work at the new 60 locations. The new locations were chosen based on an analysis of speeding accidents. The road signs on such areas will inform drivers about photo and video fixation.

Although Ukraine is applying the experience of other countries in the field of digital technologies used in the work of law enforcement agencies, we are still lack of the resources to work in this area. As a rule, there is a lack of funding from the state, there is a lack of specialists to work with new technologies and the legislation is not perfect. The use of digital technologies in the work of law enforcement agencies is an inevitable future that will definitely help and facilitate the work of the police, so the state should pay more attention to issues related to the implementation of the experience of other states in this area.

Language advisor N. V. Krasnova

UDC 351.74:001.895](100)(06)

Kyrylo DULIN

Kharkiv National University of Internal Affairs

HANDHELD LASERS USE IN CRIME SCENE INVESTIGATION

Every day, law enforcement professionals faced with unknown suspicious substances that require immediate identification before confirming the appropriate action. When criminal investigations are at stake there is no

margin for error and the demand for fast and accurate mobile techniques for the detection and identification is higher than ever before. Nowadays law enforcement agencies are using handheld lasers in crime scene investigations. Handheld laser spectroscopy devices can determine the chemical composition of an unknown substance within seconds. If an officer comes across a suspicious substance, these devices will reveal the chemical makeup almost immediately. This type of instantaneous law enforcement technology is decreasing the time officers need to be in the office or in the lab, allowing for more time in action. These lasers are also keeping officers safe from harmful substances they may not have recognized otherwise. The heavy workload of the laboratories results in unnecessary delays getting evidence to court and impacts the court's ability to set bail for a suspect. Another impetus for the use of mobile detection technologies is the lengthy time and high costs associated with laboratory analytical methods. In the case of where upon analysis, only the minority of evidence results in court submissions, the use of mobile detection technologies for sample screening would allow users to determine the identity of a substance before sending it to the laboratory for further analysis. Raman spectography is a highly selective technique and has the ability to differentiate between a wide range of compounds that is critical when faced with an increasingly broad range of threats. Unlike other handheld detection techniques, Raman analysis can often be performed through packaging material without disturbing the sample. This minimizes exposure to the operator and reduces the risk of sample contamination. Protecting evidence from contamination is critical to successful take a case to court. By allowing users to perform confirmatory analysis upon arrest and provide substantial, proven evidence, cases can proceed to court much quicker helping to reduce the backlog and increase the success rate of removing dangerous substances from circulation.

Language adviser A. E. Korshenko

UDC 351.74:001.895](100)(06)

Daria FARTUSHNA

Kharkiv National University of Internal Affairs

NEW AND IMPROVED GADGETS HELP MINNEAPOLIS OFFICERS PREVENT CRIMES

Working as a police officer used to be a career associated with routine traffic stops and piles of deskwork. However, today, all that is changed. Law enforcement technology is making its mark on police departments around the country as new-and-improved gadgets are becoming available to help officers prevent crime. There are top gadgets law enforcement officers can use to do

their jobs and make your neighborhood a safer place. In Minneapolis police departments' arsenals remote control camera robots (robotic cameras) are among the tech tools now.

Police officers cannot be everywhere at once at a crime scene, and some situations are too dangerous to risk sending officers. That is why robots have been specially designed to deploy into places officers cannot reach safely. When it is too dangerous to send a police officer into an active crime scene, or in any situation that requires "eyes" where there is no clear line of sight, police can rely on a robotic camera. The device has an electric motor and special wheels that allow it to move, climb and explore at the whim of an officer who operates it wirelessly and to keep officer out of harm's way.

The robotic cameras can be used indoors and outdoors. In Minneapolis, police use them for bomb detection by using the remote controller to drive them under vehicles to look for suspicious packages.

Driving a remote-controlled robot is no longer a childhood dream, thanks to this robotic camera. Officers can throw them into hard-to-reach areas or places without a clear line of sight and operate it wirelessly from safety. Officers are making use of this robotic technology to detect bombs or search suspicious homes and vehicles.

However, there are some special requirements when it comes to operating the device. First, officers have to be specially trained to run it. Second, when using the device at a dangerous crime scene, the operator must be accompanied by a fellow officer to cover and protect him, since his attention will be focused on the device.

Language adviser A. E. Korshenko

UDC [811.111:351.74(100)](06)

Vadim GUTSAL

Kharkiv National University of Internal Affairs

THE FUTURE OF REGULATION

As emerging technologies drive new business and service models, governments must rapidly create, modify, and enforce regulations. The preeminent issue is how to protect citizens and ensure fair markets while letting innovation and businesses flourish. Sweeping technological advancements are creating a sea change in today's regulatory environment, posing significant challenges for regulators who strive to maintain a balance between fostering innovation, protecting consumers, and addressing the potential unintended consequences of disruption.

Emerging technologies such as artificial intelligence (AI), machine learning, big data analytics, distributed ledger technology, and the Internet of Things (IoT) are creating new ways for consumers to interact—and disrupting traditional business models. It's an era in which machines teach themselves to learn; autonomous vehicles communicate with one other and the transportation infrastructure; and smart devices respond to and anticipate consumer needs.

In the wake of these developments, regulatory leaders are faced with a key challenge: how to best protect citizens, ensure fair markets, and enforce regulations, while allowing these new technologies and businesses to flourish? The assumption that regulations can be crafted slowly and deliberately, and then remain in place, unchanged, for long periods of time, has been upended in today's environment. As new business models and services emerge, such as ridesharing services and initial coin offerings, government agencies are challenged with creating or modifying regulations, enforcing them, and communicating them to the public at a previously undreamed-of pace. And they must do this while working within legacy frameworks and attempting to foster innovation.

Today, regulators face similar challenges. They must balance their charge to protect citizens with advancing innovation in new technologies and businesses, resisting the urge to overregulate. For technological innovation, regulation can be catalytic - or a hindrance. As emerging technologies evolve, regulators from around the world are rethinking their approaches, adopting models that are agile, iterative, and collaborative to face the challenges posed by emerging technologies and the fourth Industrial Revolution. To promote innovation, regulators are also moving toward creating outcome-based regulations and testing new models in sandboxes.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Viktoria HORDUSENKO

Kharkiv National University of Internal Affairs

ISSUES WITH CREDIT CARD FRAUD DETECTION TECHNIQUES

Half of all credit card fraud begins with spyware, malicious software unknowingly installed on a victim's computer or handheld device. Spyware runs in the background, collecting your data and sending it back to the criminal, who then uses your card to make fraudulent purchases. Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property.

Credit and debit card numbers can be stolen from unsecured websites or can be obtained in an identity theft scheme. Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services or to make payment to another account, which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help financial institutions process card payments securely and reduce card fraud. Credit card fraud can be authorised, where the genuine customer themselves processes payment to another account which is controlled by a criminal, or unauthorised, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party. Credit cards are more secure than ever, with regulators, card providers and banks taking considerable time and effort to collaborate with investigators worldwide to ensure fraudsters aren't successful. Cardholder; money is usually protected from scammers with regulations that make the card provider and bank accountable. The technology and security measures behind credit cards are becoming increasingly sophisticated making it harder for fraudsters to steal money.

There are two kinds of card fraud: card-present fraud (not so common nowadays) and card-not-present fraud (more common). The compromise can occur in a number of ways and can usually occur without the knowledge of the cardholder. The internet has made database security lapses particularly costly, in some cases, millions of accounts have been compromised. Stolen cards can be reported quickly by cardholders, but a compromised account details may be held by a fraudster for months before any theft, making it difficult to identify the source of the compromise. The cardholder may not discover fraudulent use until receiving a statement. Cardholders can mitigate this fraud risk by checking their account frequently to ensure there are not any suspicious or unknown transactions. When a credit card is lost or stolen, it may be used for illegal purchases until the holder notifies the issuing bank and the bank puts a block on the account. Most banks have free 24-hour telephone numbers to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on a card before the card is cancelled.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Maksym HUNKO

Kharkiv National University of Internal Affairs

NONSTOP ADVANCEMENT ON LAW ENFORCEMENT TECHNOLOGY

An advancement in information technology will enable any information of privacy concerns to be stored and if required to be shared electronically across all agencies in criminal justice. This will benefit law enforcement and police in prosecution department as well as defenders in both private and public defense bar. Today, this objective has already began to be realized. However, an efficient information system using this technology must be well coordinated and planned among the concerned agencies to avoid occurrence of technological inconsistencies. With proper planning, the police are able to work closely with the members of the community towards reducing crime as well as creating a safer community. The technology will minimize human administrative roles while at the same time increasing efficiency in management as well as accountability of all officers. In future, city agencies will easily identify and provide solutions to neighborhood problems instead of reacting to a crime long after it has been committed. The goal will easily be achieved through extensive training in order to help the citizen as well as police master skills in the use of services impacting crime as well as techniques in targeting hot spots for criminal activities.

The law enforcers have also faced high demand in data sharing with other agencies and businesses including insurance companies. Advancement in technology has also been aimed at improving police management as well as their accountability regarding probity. Technology has made the cost of crime investigation to be effective as a result of following regular procedures. Various techniques have been designed to give warning in good time for the police using force complaints. With the recent technology, police are scrutinized through internal management systems of surveillance and watchdog agencies. Therefore, enforcement technology is aimed at policing both citizens as well as police so as to make them improve their service especially in crime mapping as well as information integration. An example of application of technology since 1990 has been computer crime mapping which has been used as a tool by agencies of law enforcement. Geographical information system has been merged with mapping software and used with desktop computers in analysis of crime. Research indicates that, this technology is affordable even for police departments that operate on a constrained budget.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Bogdan KACHURIN

Kharkiv National University of Internal Affairs

THE FUTURE OF LAW ENFORCEMENT TECHNOLOGY

While many police departments have been using the above technologies for some time, some are taking advantage of newer ones. Some of the more recent technologies are still in theoretical phases, and others are for limited, case-by-case scenarios.

Predictive analytics. Much of policing involves reacting to crime or other incidents; however, technology can allow police to be proactive. Think of predictive analytics as an offensive approach to public safety. This technology takes crime mapping and data collection to the next level by predicting the general areas where future crimes are likely to occur. Information like this is helpful for assigning and distributing personnel, as one department found. “In one example cited by the National Institute of Justice, police in Richmond, VA, used data to predict where the most gunfire would occur on New Year’s Eve. “More officers were dispatched to those locations, resulting in a 47% drop in gunfire and a 246% increase in weapons seized,” reports The Press-Enterprise.

3D crime-scene imaging. 3D crime-scene imaging is quickly becoming an indispensable aspect of policing. “From quickly gathering the data at the scene to preserving it for later analysis and creating effective presentations for trials, the laser scanner is proving to be a critical tool for crime scene investigators,” according to PoliceOne. With this forensic technology, scanners capture a 3D model of a crime or accident scene, which allows for more precision of details. Officers can use this information later on to reconstruct angles and the placement of evidence or blood splatter patterns. Capturing the crime scene in 3D means officers only need to maintain the full scene for the duration of the scan, which is much shorter than usual. 3D imaging can also keep officers safer at crash sites, as less time investigating the scene means they can clear the collision sooner.

Personal, through-wall radar. Using radar to see through buildings is another way to prevent crime before it happens. The radars work like finely tuned motion detectors, using radio waves to zero in on movements as slight as human breathing from a distance of more than 50 feet. They can detect whether anyone is inside of a house, where they are and whether they are moving,” writes Brad Heath in USA Today. Though through-wall radar isn’t completely new, additions like wearable computers and augmented reality allow officers to “see” through walls and, by extension, assess threats like never before.

All in all, technology within law enforcement has created a lot of benefits that are helping different departments solve crimes, identify suspects, and track them down. This types of technologies more effective are allowing criminals to be caught and justice to be served right.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Kateryna KALUGINA

Kharkiv National University of Internal Affairs

COMPONENTS OF CYBER SECURITY RISK MANAGEMENT SYSTEM

The world digital transformation has brought increased challenges to the safety and security of digital data. Concerns over the ownership of personal data and its uses are emerging worldwide. There has been a sharp increase in the frequency, velocity, sophistication, severity, and impact of cyberattacks against companies and organizations globally. What are the best practices for protecting personal information and the integrity of digital systems while making room for the innovation promised by new technologies?

Five components of cyber security risk management system

An effective cybersecurity risk management system has five basic components, according to Steven R. Chabinsky, a White & Case partner in Washington, DC. They include:

Consideration of the specific technology risks the company faces and the establishment of priorities.

Implementation of appropriate protection in the form of technical, administrative and physical controls.

The ability to detect and properly evaluate security incidents.

The ability to respond swiftly to a breach and to bring together all sections of the company to stop a breach from worsening, while communicating effectively and while complying with any legal and contractual obligations.

The ability to recover from a cyberattack, get back to business and make sure the problem does not occur again.

The head of a cybersecurity department should be able to predict the likely impact of a breach or a hacking attack that makes sensitive data or entire networks unavailable, while it is also important to determine the implications for a brand, its operations and finances. The key, Chabinsky says, is to have adequate, business-appropriate measures in place in advance of an incident and staff trained in how to implement them. Vulnerability

scans, annual risk assessments and third-party penetration tests are extremely useful, along with written plans that are helpful for any eventuality. There are also clear benefits to ensuring the use of role-based restrictions to limit employee access to sensitive data or the ability to add or alter software, the use of multi-factor authentication to sign in to sensitive or remote systems, and the use of encryption for stored or transmitted data. Another key control is having an effective backup strategy for data that is lost or maliciously destroyed.

When it comes to detection capabilities, Chabinsky cautions that older security products are no longer a guarantee against a cyberattack because hackers constantly change their methods, and he adds that scenario-driven tabletop exercises have proved an effective learning experience for companies concerned about a breach to test their readiness to respond effectively across the organization..

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Evgeniya KALUZHNYA

Kharkiv National University of Internal Affairs

INNOVATION TECHNOLOGIES IN POLICE

Technology has become prevalent in most areas of society and, in a struggle to keep up with recent advances, public agencies are forced to innovate at an ever-increasing rate. So technology is transforming police work in the 21st century — introducing new tools to fight crime.

Adoption of such technologies is, however, not straightforward and depends upon a lot of people. And of course, the final decision on the use of certain technologies is made after the experiment «how it would work in practice».

So now I will introduce you to some modern technologies that have greatly simplified the work of the police and potentially being game-changers in fight against crime.

Firstly, Body-worn cameras. They are widely used by police in the different countries including Ukraine. And worn principally by officers in the performance of duties that require open and direct contact with the public. What helps to collect information in case of need to present it at the investigation for the presenting as evidence.

Secondly, video doorbells. They have been installed by thousands of homeowners as a way to enhance home security and give them peace of mind. And they help police automatically ask camera owners for their security footage if they live near a crime scene.

Thirdly, biometrics. Today, law enforcement officials have a plethora of biometric tools at their disposal. This wide-ranging category includes Criminal ID solutions, Automated Fingerprint Identification Systems (AFIS), Automated Biometric Identification Systems (ABIS) and facial recognition.

In conclusion, digital technology now plays a critical role in policing and security management, with policing apps, drones and body-worn cameras and other technologies that do not stop developing and help solve crimes faster.

Language adviser N. L. Gorbach

UDC 351.74:001.895](100)(06)

Mariia KANAVCHENKO

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES AT THE SERVICE OF LAW ENFORCEMENT AGENCIES

Scientific and technological progress, without exaggeration, can be considered a way of life of modern man. In Ukraine, considerable attention is paid to the development of innovation, the rapid pace of scientific and technological development of science and technology. However, in recent years, due to insufficient funding, in particular public, and due to lack of communication between scientists and customers of innovative products, the vast majority of indicators characterizing innovation in Ukraine are gradually deteriorating.

Today, law enforcement officers need a high speed of obtaining the necessary information, its accumulation and evaluation. Together with scientists from the Department of Criminology of the National Law University named after Yaroslav the Wise, a number of innovative products have been developed for the needs of law enforcement agencies, which are protected by a number of security documents. In particular, 3 patents for inventions and 8 certificates of copyright registration for works of scientific nature were obtained.

There are the following innovative outputs:

Developed by the Institute for the Study of Crime "Method of identifying a person by speech parameters" is a mathematical model of rapid wavelet transform of sound signals using quadrature mirror filters. The basis of this model are methods and algorithms that are most effective - images of signals of different physical nature. During experimental research it was found that the use of the proposed model to solve the identification of expert tasks can reduce the time for research and get more accurate results.

Created by the joint efforts of the staff of the Institute for the Study of Crime and Scientists of the Department of Criminology "Device for measuring the speed of a ballistic object" is compact, accurate, easy to use. It is very important that the surface of the ballistic object remains intact after the experimental shots. The device is recommended by the Kharkiv Research Forensic Center of the Ministry of Internal Affairs of Ukraine for use during forensic ballistic examinations.

"Automated workplace of investigator" Insight ", designed to optimize the work of investigators, judges, lawyers. Automated workplace of the investigator "Insight" is used in pedagogical and scientific activities in the field of criminology and forensic science, to improve the skills of practitioners of law enforcement agencies of Ukraine.

Employees of the Department of Criminology formed more than 30 specialized sets of scientific and technical tools for the needs of law enforcement agencies, namely:

- Universal forensic kit of the investigator;
- Forensic kit for working with traces;
- Forensic kit for working with micro-objects;
- Forensic kits "Fireman's Suitcase" and "Investigator's Suitcase";
- A set of scientific and technical means of the customs officer;
- Fingerprint suitcase;
- A set of scientific and technical tools for exploration work;
- Universal forensic kit;
- Technical set of forensic kit of the investigator;

Conclusion: Many scientific and technical tools have been developed that have improved the work of the police. This helped them to facilitate their work with traces, micro-objects and in emergency situations. This helps police officers do their job better. That is, in Ukraine, nouak-technical progress is developing.

Language adviser G. S. Babak

UDC 351.74:001.895](100)(06)

Alisa KANIUK

Kharkiv National University of Internal Affairs

NEW TECHNOLOGIES IN POLICE SPHERE

Police organizations internationally explore and experiment with new technologies to improve their performance and in response to new forms of crime.

New technologies such as artificial intelligence, big data applications, the Internet of Things, mobile internet, robotics, autonomous vehicles, cloud technology, energy storage, and 3D printing have a major impact on national and international security, producing new or different forms and targets of crime the police can improve their performance with the innovative technology. the police can identify people by biometric fingerprints. they also have a body camera with which they shoot violations. And of course new fast working cars.

In conclusion I won't to say that To cope with these new security issues and new forms of crime, the police have to move along and adapt their organization and working methods accordingly.

Language adviser N. L. Gorbach

UDC 351.74:001.895](100)(06)

Serhii KHARA

Kharkiv National University of Internal Affairs

LIVE FACIAL RECOGNITION: EXPERIENCE OF UNITED KINGDOM

Facial recognition technology is used to identify individuals or to verify someone's identity. For example South Wales Police use facial recognition technology to prevent and detect crime and help protect the vulnerable.

Facial Recognition Technology analyses key facial features and generates a mathematical representation of these features. It then compares them against the mathematical representation of known faces in a database, generating possible matches. South Wales Police uses live facial recognition (LFR). Live Facial Recognition (LFR) compares a live camera feed of faces against a predetermined watchlist in real-time. It is used to locate persons of interest by generating an alert when a possible match is found. Before using LFR, a watchlist of offenders is created, that are wanted by the police and courts. The watchlist also includes people who may pose a risk of harm to themselves or others. An officer then compares the camera image to the person they see and decides whether to speak to the person. Persons who are not included on a watchlist cannot be identified. Live Facial Recognition technology is considered an efficient and effective policing tactic to prevent and detect crime, and protect the most vulnerable in our society. Police typically use the technology at public events and crowded public spaces. South Wales Police do everything reasonably possible to inform the public where they are using Facial Recognition technology for example:online before it is used, South Wales Police website where the results are published

of when LFR is used, posters and signs to include QR codes to make people aware LFR is being used and where they can go to find further information and police officers are available to explain to the public how LFR works and why they are using it.

There are many benefits facial recognition can offer society, from preventing crimes and increasing safety and security to reducing unnecessary human interaction and labor and it is obvious that Ukrainian police should further implement such technologies in their everyday work.

Language adviser N. V. Krasnova

UDC 351.74:001.895](100)(06)

Maxim KHARCHENKO

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN POLICE

Police innovation is frequently referenced in the policing literature, but it is less frequently defined, applied, or operationalized by scholars. This situation has led to definitional ambiguity and variation, which limits the development of innovation as a scientific construct. Chiefs also appear to classify innovativeness in terms of the utility that innovations provide to organizational operations.

Probably, many people have seen a video in which drones chase quarantine violators, urging them to return home. On the one hand, this looks funny, but the use of drones in the work of law enforcement agencies greatly facilitates the supervisory, investigative and even law enforcement activities of the police. For example, unmanned aerial vehicles (UAVs) more accurately capture scenes of criminal offenses, perform the functions of rescuers, monitor public places, collect data using GPS technology, which is then used for criminological and forensic research.

Of course, drones are far from the only "wow-efficiency" innovation used by law enforcement to better protect the population and maintain law and order. But it's worth learning more about.

Drones. The topic of unmanned aerial vehicles is difficult to exhaust in a few introductory paragraphs. Their use causes many legal and security controversies: from the most obvious violation of privacy to the use of drones for reconnaissance and military purposes and the violation of air borders.

In 2018, CNN published an article on the use of drones by the largest police department in the United States - the New York Police Department. According to the head of the department Terence Monegan, the use of UAVs

is necessary in emergencies, and therefore violations of privacy are not expected. However, human rights activists and citizens do not support this opinion.

According to a March 2020 report by the Bard College drone research center, about 102 countries use UAVs for military purposes. In the field of law enforcement, about 1,578 state and municipal institutions use drones.

As for Ukraine, the UAV is used by the water police to identify violators of the quarantine regime, the EU Advisory Mission trains forensic departments of the National Police in the use of drones, and the problem of burning leaves, which this year turned into a tragedy, tried to solve in 2018 with UAVs.

Predictive policing. Redictive policing is a very promising practice of using artificial intelligence in policing. Imagine a world where police are waiting under an offender bank building before a robbery occurs. It sounds like a utopia, however, based on the collected and processed big data, such a prospect is quite probable.

The technology was first discussed in 2008 when Los Angeles Police Department Chief William Bratton began developing crime prevention methods with the support of the Bureau of Justice Assistance and the National Institute of Justice.

The forecasting method itself is classified, however, from general sources you can get an idea of what parts of the data are to be collected and processed: the history of crimes in a particular area (usually a small area, like parts of the city); collection of characteristics of previous offenders; data collection from video surveillance systems; assessing the potential of individuals to commit certain types of crimes; urban assessments; the frequency of accidents in a particular area; material security of the residents of the study area, etc.

Robots and self-driving police cars. Usually, when we hear the word "robot", we imagine a human-like cyborg who either wants to take over the world or wants to get the citizenship of Dubai. However, the works are less humane and functional. However, this does not prevent them from preventing the commission of crimes or their socially dangerous consequences... Sometimes in rather strange ways.

The patrol police, when resorting to police measures, in particular to stopping vehicles, may encounter an inadequate and sometimes dangerous reaction from the driver. In the United States, where the carrying of a weapon is a constitutional right of an individual, such cases are not uncommon. That's why a traffic stop robot was invented - an analogue that can act instead of a real person and reduce the risks of using firearms. Functional work includes scanning of drivers licenses, issuance of penalty receipts, detention of drivers by means of "spike arm".

Also worth mentioning are the bomb-deactivating robots (the ancestor of which is the ex-lawn mower with the Wheelbarrow remote control, invented in 1972), self-propelled police cars (I recommend reading the controversial views on this account in the work of Andrew Gregg) and even about potential substitutes for human policemen, such as AnBot robbers.

The use of robots in law enforcement is not just an innovative pastime. It is an opportunity for the state to save on pension and other social benefits paid to law enforcement officers, the opportunity to protect police officers from occupational injuries and save their lives, and finally - to increase the effectiveness of preventive, preventive and law enforcement measures.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Violetta KIRIIENKO

Elizaveta ZAGORETSKA

Kharkiv National University of Internal Affairs

ECOLOGICAL CRIMINALITY IN UKRAINE AND FOREIGN COUNTRIES

There are about 200 countries in the world. They have a different level of economic development, different state of welfare, have different approaches to solving environmental problems. At the same time they share the responsibility for preserving and renewing the favorable state of the environment for the benefit of today and future generations. Let's briefly review the experience of the law of the environment in economically developed countries.

The approach of Spanish criminal law to the problem of conservation of flora and fauna is noteworthy. Art. 334 The Spanish Criminal Code provides for liability if a person destroys species threatened with extinction as a result of hunting or fishing, as well as carry out activities that disrupt or hinder their reproduction or migration, violating the laws or general provisions for the protection of species of forest animals. This norm prohibits trade or transportation of these species or their remains. Such actions are punishable by imprisonment for six months to two years or a fine of eight to twenty-eight months wages.

On the 18th of November 2000 the French Environmental Code was adopted. The law is ranked first in the hierarchy of domestic law after the Constitution. The French Environmental Code consists of General and Special Parts (975 articles). The General part includes principle, goals and environmental responsibility. The special part regulates the protection of

nature, water and air. According to the French Criminal Code of 1992, criminal liability for environmental offenses is borne by all legal entities, except for the state, administrative and territorial entities and its associations. The main types of punishment for them are fines and limitation of their activities. The maximum amount of the fine imposed on the legal entity is equal to nine times the amount of the maximum fine imposed on the natural person.

Under U.S. law, a criminal fine of up to \$25,000 per day of violation, or imprisonment up to one year, or both, may be imposed for a criminal violation of specific provisions of the Water, Air, and Waste Management Act. In case of repeated violation - a fine of up to \$50,000 per day of the violation or imprisonment for up to 2 years. Criminal responsibility for environmental offenses in the United States is imposed for a criminal violation of the law.

One of the most environmentally friendly countries in the world is the United Arab Emirates. The new UAE Code, which is entirely dedicated to environmental offenses, includes 105 articles and reportedly includes penalties for water pollution, soil pollution, damage to nature reserves, green spaces, and so forth. For a particularly grave crime against nature - the contamination of nuclear waste - the Code may consider the possibility of conviction.

So a comparative analysis of foreign legislation on environmental protection is very interesting to study, and the positive experience can be used to improve the Ukrainian legislation. Some legislative norms are of particular scientific interest and deserve follow-up, for example, the introduction of penalties for persons who report cases of poaching, introduction of norms stipulating the liability of legal persons for environmental crimes (e.g. France, the USA), adoption of the Environmental Code. On the basis of analysis of the current legislation, Ukrainian and foreign legal experience in the sphere of ensuring the implementation of the right to favorable environmental conditions it is necessary to enshrine this laws in the Ukrainian legislation as a law-guarantee, as well as social, economic and other laws of citizens.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Svitlana KOBYLINSKA

Kharkiv National University of Internal Affairs

FIVE INNOVATIVE POLICE TECHNOLOGY IN ISRAEL

Technology is transforming police work in the 21st century — introducing new tools to fight crime and new categories of crime to fight. The Israeli police are keeping pace with the times, actively applying innovative technologies in their work.

An exhibition is expected to be held in Tel Aviv to coincide with the start of the Second International Conference on Internal Security, during which the Israeli police will showcase new developments to help law enforcement officers fight crime.

The Israeli police will present a range of innovative technologies, including:

- "Eyeballs" are miniature video cameras the size of tennis balls that can rotate and receive 360-degree information. In addition to being smaller, less cumbersome, and more durable, some cameras are designed to better integrate with in-car systems to provide synchronized video of an event from multiple points of view. Other advancements include higher resolution, clearer audio, wider fields of vision, and heightened resistance to environmental conditions such as extreme cold.

An innovative shooting simulator that offers police officers the opportunity to significantly improve their skills in handling weapons in a variety of computer-generated situations.

- Unmanned Aerial Vehicle. Drones are increasingly being used by police to obtain aerial vantage points for crime scene work, search and rescue, accident reconstruction, crowd monitoring, etc. Israel introduces a balloon used for aerial surveillance, has a volume of only 3 m³ (instead of the previous 20 m³), which fits easily in the trunk of a car, and is controlled from the ground using a special kind of smartphone.

- Voice Technology. One of the latest innovations being incorporated into police cars is a new voice command technology that empowers officers to control many functions in their vehicle while driving and performing other patrol duties. The capabilities of these voice systems vary from vehicle to vehicle, but most can handle commands to run a license plate or turn on a siren. The more advanced and most promising capability of voice command technology in police cars will make filing reports much easier — officers can dictate their notes which are then logged directly into their agency's system.

- Automatic License Plate Recognition (ALPR). The same technology that allows toll collectors to automatically scan and collect registration numbers and letters on your license plate to charge you is now being used by police for various law enforcement purposes. The fact that multiple cameras can capture images of the same license plate potentially gives police the ability to track the movement of a vehicle over time, revealing details about the operators whereabouts, which can certainly help in catching criminals.

This is not all that can surprise Israel, so it is safe to say that police technology is evolving and not standing still.

Language adviser **G.S. Babak**

UDC [811.111:351.74(100)](06)

Kateryna KORZH

Kharkiv National University of Internal Affairs

THE ADVANCEMENTS IN LEGAL TECHNOLOGY FOR THE CRIMINAL JUSTICE SYSTEM

Legal technology for the criminal justice system involves GPS systems, robots, advanced cameras. The high-performance computer systems and Internet technologies are also involved. All these technologies improve surveillance and investigation while making analysis procedures easier. Computer programs have incorporated themselves into almost every facet of law enforcement. They are associated with different jobs, ranging from robotic cameras to DNA testing. The number of electronics and new technologies in criminal justice is rapidly growing. And they all have the same goal – to make the jobs more effective. But this is a two-edged sword, as the criminals also make use of these technologies. They abuse technology for illicit usage. There are more and more tech-savvy criminals these days. That's why experts in criminal justice have to keep a step further in this "technology combat." Despite all these advanced technologies, It happens that someone is unjustly accused. This is where a defense criminal lawyer comes in. A lawyer has to advocate vigorously when protecting the rights of accused persons.

There are some unique forms of legal technology for the criminal justice system. They include different positioning and detection systems, such as: GIS and GPS systems - these systems have been around for years in the police. The officers use them for different purposes. When identifying a suspect location, getting the most effective routes, and so on. Gone are the days when police officers had to engage in a high-speed, dangerous chase. GPS help them track criminals much easier today. Likewise, GIS systems track police vehicles. That helps departments determine their location at any moment; Gunshot detection systems (GDS). The police often install the systems of electronic sensors in high-crime areas. That helps them detect where a gunshot comes from. This way the officers have a better response time; Robotic cameras, robots, and drones. The robots can replace the officers in many dangerous situations. Thus, they can check out the hazardous areas, diffuse the bombs, and the like. Apart from terrestrial robots, there are also flying drones. Those devices provide a bird's eye view, which is beneficial for many crime scenes. They are especially useful in hard-to-reach places; Automatic License Plate Recognition systems. Many police cars are equipped with the cameras that can capture license plates with ease. This allows the officers to see at once if a car is stolen or not. And the list of legal technology for the criminal justice system goes on. There are also body-worn cameras,

through-the-wall radars, predictive analytics software, and so on. While some are not completely tested yet, other devices are pretty controversial.

Law enforcement agencies across the world are recognizing the value of those tools. More and more departments use the new technologies for everyday activities. Yet, many still have to learn how to use software and computers more effectively. That will set them up for success in their future careers.

Language adviser I. O. Gogol

UDC [811.111:351.74(100)](06)

Olena KOSTENKO

H.S. Skovoroda Kharkiv National Pedagogical University

LABOUR EDUCATION AS AN EDUCATIONAL INNOVATION AIMED AT CREATING SAFE SOCIAL ENVIRONMENT

Considering the modern challenges faced by our country, it is necessary to pay special attention to creating a safe social environment. In this context, the educational process becomes crucial as it forms new members of society.

One of the methods of educating a harmonious personality is labour education. Despite the fact that this method is historically well known, nowadays in Ukraine it can be considered as a pedagogical innovation, due to the fact that it has not been used in practice for a long time.

The history of Ukrainian pedagogy knows well the pedagogical heritage of Sofia Rusova, Konstantin Ushinsky, Anton Makarenko, and others who used elements of labour education in their pedagogical practice. In this work, the author proposes to consider foreign historical experience of labour education, based on the ideas of enlighteners about the comprehensive development of the individual, equality and the rule of law.

Among the foreign apologists for labour education, J. Locke, G. Pestalozzi, K. Bazedov, M. Montaigne, I. Fichte could be named. The vision of labour of each of them has its own characteristic features. All of them underline the creative function of labour. It should be directed to the formation of a fully developed personality. Via education, having become a part of the human social habitus, labour helps to cope with negative behavioural patterns.

As a pedagogical innovation, labour education can imply active inclusion of elements of labour in the educational process, starting from a very early age. At the same time, it is necessary to observe strictly the principle of compliance with the level of complexity, voluntariness, understanding the significance of the tasks performed. Maintaining student

interest is essential. All conditions having been taken into consideration, the method of labour education could help to educate a comprehensively developed personality, who will be accustomed to work. This, in its turn, will contribute to the creation of a safe social environment.

Language adviser Tetyana Chudovska

UDC 351.74:001.895](100)(06)

Dmytro KOVAL

Kharkiv National University of Internal Affairs

DNA SAMPLES USE FOR CRIMINAL INVESTIGATION

The Australian Federal Police (AFP) are utilizing a new technology that opens a new world of forensic DNA testing for criminal investigations. The new technology is known as Massively Parallel Sequencing (MPS) can provide predictions for visual traits of criminals from the DNA they leave at a crime scene allowing investigators to predict gender, biogeographical ancestry, eye color and, even, hair color. Biographical ancestry prediction compares DNA to a reference library of three ancient human population groups, which may help exclude persons of interest. The AFP has been carefully testing and assessing MPS to ensure its accuracy, prior to any use in forensic investigations. This validation for use in forensic analysis is an Australian first for law enforcement. MPS works by examining the nucleotide base sequence of the DNA that is present in samples collected at a crime scene, this is the fundamental code for all living things including humankind.

Current DNA profiling technologies for human identification examine the length variations on the human genome, but MPS examines the nucleotide sequence of those regions, making MPS more informative than traditional DNA profiling.

The true power of MPS technology comes from its ability to obtain leads from DNA when the perpetrator is unknown and there is no matching profile on a law enforcement DNA database. The platform also has application in missing persons and unidentified human remains cases. The AFP is also currently collaborating with academia and Geosciences Australia to develop MPS capabilities to analyze environmental DNA as a forensic tool for soil, dust and water profiling and drug investigations.

Over the next decade prediction capabilities will be widen to include traits such as age, body mass index and height. There will also be seeking opportunities to provide fine detail predictions for facial metrics such as distance between the eyes, eye, nose and ear shape, lip fullness, and cheek structure.

The AFP is also mindful of maintaining public trust and confidence in the use of new biotechnology, and has implemented processes to minimize privacy impacts and to safeguard any genetic information.

Language adviser A. E. Korshenko

UDC [811.111:351.74(100)](06)

Bozhena KOVALENKO

Kharkiv National University of Internal Affairs

INNOVATION TECHNOLOGIES IN POLICING

Now, in the 21st century, in the age of technology. The police are also not standing still, but are developing by introducing something new. For example Automatic alerts, Body cameras and DVR. They help the police do their job well. Automatic alerts reduce response time

Law enforcement officers cannot react faster than the system that supplies them with information. With networked video and audio solutions, police officers can be notified of incidents almost immediately, significantly reducing response time. Network cameras - with integrated analytics, sensors and alarms - monitor high crime areas or where citizens feel threatened and send automatic alerts as situations develop. Incident detection and live video from the scene will help you understand the true nature of incidents and prioritize accordingly. By integrating loudspeakers and spotlights into the network, you can even stop crimes and offenses right at the time of their commission. Body cameras allow you to collect valuable evidence. And this, in turn, will effectively prevent unwanted behavior and have a positive impact on the actions of camera carriers and the public. A smart video surveillance network not only helps prevent crime, but also helps increase conviction rates and bring criminals to justice. The operations center provides officers with all the information they need before they even arrive on the scene. By knowing what to expect and what to look out for, the police on site will be safer; moreover, it will dramatically increase the chances for further successful work of forensic specialists. Smart analytics (such as license plate recognition and facial recognition) can also make a decisive contribution to investigating crimes and apprehending suspects. Video surveillance footage can also be used in court.

The latest technology makes police work faster, better and more independent..

Language adviser I. O. Gogol

UDC [811.111:351.74(100)](06)

Elizaveta KOVALENKO

Kharkiv National University of Internal Affairs

ROLE OF TECHNOLOGIES IN INDIAN CRIMINAL INVESTIGATION

Technology has revolutionized the world we have been living in. From every instance of opening our eyes in the morning, technology starts playing its role. In fact, after the black swan event, almost everything has been digitized. From education, shopping, food delivery, transportation, and banking transactions, and even the offices have shifted to homes because of the drastic and far-reaching effect of technology. Technology has changed every aspect of life drastically. In such a fast-moving world of technology, it is imperative for our police in criminal investigation to buckle up and use technology to keep up with the current state of affairs. The police have already incorporated many technological aspects but there is a need for up-gradation every now and then.

Due to the advancement in the world and in steep growth in the field of technology, it is important for the police to adapt to the changing world. With the changing world, crimes have also evolved and have taken a new form like cyberbullying, theft of money, data theft, ransomware, website spoofing, IoT hacking, etc. With the ever-increasing crimes in India coupled with such a low population-to-police ratio, it is necessary to have the technology to fill the complexities and make timely decisions. Information and Communication Technology is the method to provide sophisticated services by merging information technology and telecommunication. ICT is used to store, retrieve, analyze the data. It also includes a mobile phone, video conferencing, etc. These technologies are being used efficiently by the police for law enforcement and can be constantly improved for good governance.

The use of technology can be of great help in fair trials. In today's time of the coronavirus pandemic where social distancing is advised, it is extremely dangerous to go to a crowded court. However, because of this pandemic, many cases could have remained pending, the piles of case files would have mounted. But, technology came to our rescue. The court trials are even continuing in this pandemic due to the facility of video conferencing.

In the present era, we cannot imagine a day without the appropriate technology. It is a dire requirement even in the criminal investigation by the police that new technologies be incorporated. Many technologies are already in use but constant up-gradation is required. Technology has been a boon but there have been instances where gross misuse of these technologies has been

carried out. For the prevention of such instances, it is imperative to formulate legislation. Technologies are costly and therefore, we should focus on research and development in our own country.

Language adviser I. O. Hohol

UDC [811.111:351.74(100)](06)

Oleksandra KOZLIANSKA

Kharkiv National University of Internal Affairs

ADVANCEMENTS IN THE FIELD OF CRIMINAL JUSTICE

According to the Sayre Davis from Southern Utah University, criminal justice is a rapidly developing career field. Every country in the world needs employees in this field and that need will never fade. As technology has been advancing in the civilian world the technology in the criminal justice world is also advancing. Here we will discuss brand new technologies almost only used in the criminal justice realm. However, we will not talk about how civilian apps and technology such as social media are being used in law enforcement, yet they are essential to be aware of if you are considering and studying this topic. The few we will discuss are the online cloud systems, new detection abilities, advances in DNA testing, pre-crime technology, improved protection, and artificial intelligence.

Online Cloud Systems. One of the most effective advances in the criminal justice system is the development of online cloud systems which share information with other employees, as well as other cities and states in an instant. The old way of writing everything down and storing it in files is becoming less commonplace.

DNA Testing. The development of DNA testing has changed the way that the industry operates. DNA was once not available to help with crimes which left many cases unsolved. Now that this is commonplace advances in DNA testing are coming quick.

Detection Abilities. One of the most important steps for law enforcement to do their job well is the ability to identify and detect crimes sooner than later.

Improved Protection. The need to protect law enforcement officers is a growing concern due to civilian technologies progressing including in the field of firearms and other weapons. One of the fastest-growing and used improved protection is the “smart belt”. The smart belt has a system that alerts dispatch and other officers if a gun, or other tool, is drawn out of the belt. This tool would allow faster backup, allowing officers to have safer exchanges as well as to be protected by lawsuits and other things.

Artificial Intelligence. In law enforcement, the most commonly found artificial intelligence (AI) is built into the databases they use. These AIs compare crimes, past criminal records, locations, license plates, and much more to try and help law enforcement pinpoint criminals. Many of this artificial intelligence is becoming more effective and helpful.

The criminal justice system is changing and becoming more adaptive to the current world. With advances like online cloud systems, new detection abilities, advances in DNA testing, improved protection, and artificial intelligence, the criminal justice system is more effective and efficient than ever.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Yana KRAVCHENKO

Kharkiv National University of Internal Affairs

COMPUTER FRAUD AND CYBER CRIME IN SOUTH FLORIDA

Recently the emphasis of South Florida law enforcement has been the seizing and holding of personal computers of those under investigation for computer fraud or cyber-crime. In their race to combat computer fraud and cyber-crime, police have occasionally been found conducting illegal searches and seizure of personal computers and other related property. That why they explane a difference between Computer Fraud or Cyber Crime.

Computer Crime pertains to criminal acts that are committed through the use of a computer.

Cyber-crime and Internet crime usually involves the use of a computer and the Internet or cyber space.

Computer crimes, cyber-crimes and Internet crimes can be “pre-computer” crimes that existed before the advent of the computer, such as: embezzlement, fraud, financial scams, identity theft, stalking, etc.

They can also include “modern technology” crimes that began with the introduction of personal computers, networks, cyberspace, and the Internet: hacking, phishing (smishing: SMS texting and phishing; vishing: voice and phishing), pharming, spam, software piracy, information warfare, viruses, worms, denial-of-service attacks, Trojan Horses, Bots, Malware (malicious code), e-scams, cyber-stalking, cyber-bullying, online predators, drug trafficking, etc.

Computer crimes, cyber-crimes and Internet crimes include various categories of criminal activity. The U.S. Department of Justice classifies cyber-crime into 3 basic categories:

1. The crime of illegally obtaining computer hardware and software;

2. Crimes that directly target the Internet (chat rooms, e-mails, notice boards and groups), computer networks, the “cloud” or mobile phones (ie: computer hacking, viruses, worms; any unwanted intrusion into an electronic device) and

3. Crimes committed through the use of the Internet, computer networks, the cloud or mobile phones (ie: fraud and identity theft, phishing, pharming, e-scams, embezzlement, software piracy, music piracy, movie piracy, cyber terrorism; child pornography, international espionage, financial theft, etc).

In any case, prevention, detection, and mitigation are all part of protecting your identity and maintaining good standing in the financial arena. Reporting the theft and fraud is the first step to mitigating and or minimizing damage.

Language adviser A. V. Bilousov

UDC 351.74:001.895](100)(06)

Oleksandra KULAK

Kharkiv National University of Internal Affairs

MOBILIZING TOOLS FOR FUTURE POLICING STRATEGY

Good policing strategy and technology are aids to core policing. One will be of no use without the other one in a time like this. With the evolving law enforcement policies, it is crucial to acknowledge the pace at which the technology is evolving too. With the help of the technology, the core aspect of how the public reacts to the different strategies and tools used by the law enforcement bodies to control the criminal activities determines the efficiency of the new tool in our society and whether it would work or not.

For example, there is an app used in the US known as US Department of Justice NSOPW App which detects registered sex offenders in the radius around you and that is a very helpful tool to keep the police as well as the general public aware of their surroundings. On the other hand, even though some states have a sex offender registry but the police have not made it public yet. The secretiveness of the police to protect the privacy of sex offenders is a disadvantageous strategy for the community. The above-stated example also shows that the police need to adapt themselves with the new strategies and policies that can meet the challenges of the evolving crime rates around us.

A distributing virtual and sensing patrol is one more technological mean. Using technology and putting efforts to obtain substantial results rather than investigating dead ends without the proper equipment will not only save time and energy but will also deteriorate the number of crime rates around us. Even if separate departments are created with an equal workforce to prevent crimes, the possibility of being physically present at the scene of the crime when the

crime is happening is next to impossible. Therefore, technologies such as the Internet of Things (the concept of a computer network of physical objects equipped with built-in technologies for interaction with each other or with the external environment), smart sensors, security cameras are the need of the hour. With lesser man force and more technology, the police can still keep an eye on the society and allow access to unparalleled awareness. These commodities can provide raw data that would be used for detailed studies and analysis to make the investigation quick and efficient.

The technologies should be smart enough to assist the police officials on the physical crime scene. Tech devices like the electronics miniaturization, 5G communications, AR Glasses, surveillance drones, etc. allows the police to open up various proofs that can go unnoticed for human eyes. Things like previous call logs, locations, crime history registry, etc. are some examples of things that are used to strategize and execute raids, missions, etc. The perks of new technology also include digital back up in the field. In simpler words, drones and cameras are used on fields as a security backup.

Language adviser A. E. Korshenko

UDC 351.74:001.895](100)(06)

Oleksandr KURILKIN

Kharkiv National University of Internal Affairs

CHANGING POLICE ECOSYSTEM FOR A SAFE FUTURE

We live in a world where the crime rates go up every single day, where humanity is questioned after every act of crime happens, where the gravity of the crime is shooting up in the sky, where stricter law enforcement policies are more important than the religious squabble we observe around us. In a world like this, new methodologies, technology, and new ideas are the need for the hour. The law enforcement agencies began with taking up new ideas, technologies, etc. were embarrassed with new concepts introduced to the world of crime. The need of the hour is changing police ecosystem for a safe future.

Law enforcement bodies were created to make sure that every citizen abides by the rules and regulations so that the eventual result would be to keep society safe and the world a better place to live in. New technologies do not only mean technological advancements. The new strategies, plans, ideas, methods, etc. to form an essential part of the new developing technologies. New technologies can only be enforced if the police have a sense of selfless community services, a sense of responsibility, sacrifice, and morally stable integrity. In today's tech-savvy world, the advancements are tearing the roof

daily by inventing new technological devices and services daily. Along with the code of ethics, the law enforcement body needs to enjoy the new developing environment around them with dynamic enthusiasm and a realistic action strategy to shape the society towards a new, different and positive direction.

New strategies need to be formulated while keeping in mind the impact of both proactive as well as reactive policing on the community and the crime. For example, weapons buyback programs. The program includes the inputs of the community as the person who returns lost weapons back to the police receives a cash reward. Firstly, this program was enforced to convict all the illegal weapons off the streets and at the same time engage the community into making their surroundings and community a safe place. Lack of fundings for the equipment, weapons, technology, etc. results in the deterioration of the investigating standards. Investigations are tampered with due to the lack of organized communication between the various departments. Modern technology is not used as much due to the lack of skilled police officials that eventually deteriorates the training standards too. The media has been very vocal to express its disappointment towards the super ineffective accountability that the police tend to bring into the play of policing. Hence, it is very necessary to bring about a change in the police ecosystem that will generate a safer environment for everyone.

Language adviser A. E. Korshenko

UDC [811.111:351.74(100)](06)

Maksym KUSHCH

Kharkiv National University of Internal Affairs

USE OF THE LATEST FORENSIC TOOLS AND INNOVATIVE TECHNOLOGIES

To a large extent, the effectiveness of law enforcement depends on technical equipment and the use of innovative technologies in the professional activities of police officers. Thinking about future forms become starting points in the organization of tasks and technical ideas. This is especially true for the innovative vector of development, which requires law enforcement agencies to take a new approach to the performance of official duties aimed at protecting human rights and freedoms from unlawful infringements.

The use of the latest forensic tools and innovative technologies certainly contributes to the optimization of police activities in the fight against crime. Local networks and automated workplaces are created, which allows to release practitioners from performing monotonous operations, provides the

possibility of simultaneous consideration of a significant number of facts in interrelation and dependence while processing a variety of information. Foreign experience in the use of innovative technologies in the professional activities of police officers deserves special attention.

The use of innovative technologies in the work of the police of foreign countries can be divided into two main categories:

- tangible technologies (hardware or materials);
- intangible technologies (computer software, information search systems).

Currently, a significant number of innovative companies are developing mathematical algorithms and video cameras for three-dimensional (3D) or combined (2D+3D) human face recognition images. The video surveillance system of modern cities is a major component of an integrated security system. Video images are an important source of objective information about the situation, allowing you to make the right decisions in ever-changing situations in the dynamics of ever-changing situations.

To summarize, we can say that information technology in the field of communication, information processing, compilation of data used in the service of law enforcement agencies of foreign countries will soon become the basis of the era of a new digital investigation of criminal offenses. Law enforcement agencies are constantly expanding sources of information acquisition and processing, actively use information systems to search, storage and delivery of the new generation of accounting data

Language adviser G. S. Babak

UDC 351.74:001.895](100)(06)

Kateryna KUZNICHENKO

Kharkiv National University of Internal Affairs

CLOSED CIRCUIT TELEVISION CAMERA AS A CRIME PREVENTION MEASURE

Closed Circuit Television (CCTV) surveillance has emerged globally as a mainstream crime prevention measure. This technology is already present in many public places such as railway stations, airports, office buildings and on the street. While CCTV cameras were formerly employed as a means to report crime, support police officers with prosecution processes or as supporting evidence in court of justice. The developments in computer vision and machine learning provide opportunities for investigating CCTV surveillance as a crime prevention mechanism. CCTV cameras are typically intended to reduce crime through several mechanisms.

The first is to deter offenders who fear being identified committing a crime on camera.

The second is to provide law enforcement agencies with an opportunity to identify crimes in progress or those that are about to happen, to provide them with an opportunity to intervene.

Where these two mechanisms fail, CCTV cameras can record evidence that a crime occurred, who was involved and what took place, which can be used in criminal prosecutions.

The first mechanism relies on offenders perceiving that CCTV is effective, otherwise there will be no perceived risk.

The second relies on staff monitoring camera feeds and being able to identify suspicious activity.

The third relies on the camera being able to capture an event in progress, which may require it to pan and tilt accordingly.

Language adviser **L. S. Sazanova**

UDC [811.111:351.74(100)](06)

Diana KYRYCHEKO

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES FOR THE USE OF DRONS IN SWEDEN

Known worldwide as one of the most progressive and happiest places on earth, Sweden is the fifth largest country in Europe. From year to year the quality of life in Sweden is estimated to be much higher than in other countries. This is largely due to the fact that the Swedish police play a major role in reducing crime and improving public safety.

In 2015, the Swedish Police Administration became the central governing body of the Swedish police. This was a notable change after decades of controlling municipal government. Already one of the leading countries in the application of new technologies to protect the public, Sweden has begun to study the use of drones.

The country has officially launched a program to use police drones in 2018. Police officers from each department were given the opportunity to participate in a training program and receive training to use drones in the line of duty.

Sweden is perhaps the largest drone program for public safety in Europe. Given the successful work of the Swedish Police Department in conducting operations to maintain public safety with the use of UAVs, this progress seems quite natural.

For example, sending drones for photography and video to crime scenes or events has helped the police reduce the risk of losing evidence. Police drones also assist fire services in rescue operations and reconnaissance in the event of fires, oil spills and natural disasters.

Moreover, Sweden uses drones to provide security and control the crowd during large mass events such as football matches, election rallies and demonstrations. Thanks to new technologies, it has become easier to search for the missing in the mountains or at sea.

Drones often fly in public places in disadvantaged areas, where the number of cases of drug trafficking and offenses committed by criminal groups increased in 2019. These drones, which have complemented the foot patrol and other security measures taken by the police, have made it easier to prevent and detect crime. Police officers care about the privacy of citizens, so they have the right to use aerial photography for investigation and prosecution. Aerial photographs and videos provided as material evidence in court are often a decisive factor in cases without witnesses. This provides safer working conditions for law enforcement and rescue workers.

Public safety work often requires immediate decision-making, so permission can be obtained when the police arrive at the scene. After obtaining permission to use drones, the pilot must inspect and follow the steps described in the user manual. The response team must also submit to the office a detailed report describing each flight.

Language adviser G. S. Babak

UDC [811.111:351.74(100)](06)

Kyrylo MAKARENKO

Kharkiv National University of Internal Affairs

«DRONES AND ROBOTS IN UNIFORM: HOW TECHNOLOGY CHANGED THE POLICE»

The average annual growth rate of global law enforcement spending on software and equipment is 9.3%. In 2018, funding was estimated at \$ 11.6 billion, in 2020 more than \$ 13.6 billion has already been spent, and by 2023, according to the estimates of the analytical company, the budget will increase to \$ 18.1 billion.

In the USA, a mechanical engineer at SRI International, a California research institute, has designed a robot to help police officers avoid potential conflicts with motorists.

The robot can scan the driver's documents and issue a fine, and so that he does not leave, it unfolds a bar with spikes under the wheels of the car. At the

same time, the policeman may not leave the car in order not to put himself at risk.

So far, the novelty is undergoing tests.

Another assistant system will soon be available for UK police. With the help of it, law enforcement officers plan to predict the commission of serious crimes of a violent nature using artificial intelligence technologies.

The National Data Analysis Solution (NDAS) uses a combination of artificial intelligence and statistics. To search for “future” criminals, the system assesses more than 1.4 thousand characteristics. Artificial intelligence algorithms calculate a person at risk and assess the likelihood of committing a crime with the use of a weapon.

In India, startup Staqu is also developing a range of assistive technologies for law enforcement, such as ABHED (Artificial Intelligence Based Human Efface Detection), an application for fingerprint, face and voice recognition.

Another development of Indian scientists - "smart" glasses based on artificial intelligence, which will help the police to identify potential criminals in real time. They are equipped with cameras that take pictures of people and check the pictures against a database of criminals. If a match is found, the information will be displayed on the built-in projector.

Body-worn cameras

Body-worn cameras are mobile video recording devices. Such equipment was actively used during the 2014 riots in Ferguson, Missouri. Then, under pressure from the public,

USA President secured an investment of \$ 263 million to purchase cameras that will increase the transparency of police interactions with citizens.

Shot locators

Optical and acoustic sensors with geo-position recovery allow you to track the shooting. For example, ShotSpotter technologies are used by more than one hundred cities in North America and South Africa.

To conclude, one can say that the purpose of this work is not to replace professionals with artificial intelligence, but to create a modern tool for them that will increase the productivity of employees and reduce labor costs when conducting legal and anti-corruption examinations.

Language adviser G. S. Babak

UDC 351.74:001.895](100)(06)

Mykola MAKOVCHYK

Kharkiv National University of Internal Affairs

CHINA'S POLICE NEW WEAPON IN SURVEILLANCE

A new surveillance was designed in China to identify people by how they walk, or the shapes of their body. Besides, a great number of surveillance cameras which use bleeding edge optics and facial recognition technologies already use the tool on the streets in its two largest cities, Beijing and Shanghai. It raises concern among privacy advocates about how far the government is willing to go to keep tabs on its citizens.

The company that designed the system says it can identify people from up to 50 meters (165 feet), even when their back is turned or their face is covered. Chinese facial recognition glasses are a dystopian nightmare come true.

Each set of facial recognition eyeglasses is equipped with optics and advanced facial recognition algorithms capable of pinpointing a single fugitive in even the most crowded places like a train station or airport.

The glasses automate the process of identifying passersby, in seconds and without unparalleled accuracy. When the wearer looks in someone's direction, the attached camera takes precise measurements of the width and depth of a face before comparing it to a database of identified individuals.

Police officers in Zhengzhou have been spotted wearing sunglasses equipped with facial recognition software that allows them to identify individuals in a crowd. China is a leader in the development of artificial intelligence (AI) for surveillance. The country's closed-circuit television (CCTV) system tracked down a BBC reporter in technology just seven minutes during a demonstration.

Language adviser L. S. Sazanova

UDC 351.74:001.895](100)(06)

Dmytro MALIARENKO

Vladyslav SHUVALOV

Kharkiv National University of Internal Affairs

INNOVATIVE POLICE TECHNOLOGIES

Technology is transforming police work in the 21st century — introducing new tools to fight crime and new categories of crime to fight. For example, police departments are deploying drones as eyes in the sky or they use body-cam to film their work in action etc.

Facial Recognition Software. One of the more controversial emerging police technologies involves the use of facial recognition software. When this tool first made its way into law enforcement repertoires, many were concerned that it would be used unethically. Thankfully, that has not been the case, and facial recognition is proving to be an effective investigative tool.

Biometrics. Police have been using fingerprints to identify people for more than a century. Now, in addition to facial recognition and DNA, there is an ever-expanding array of biometric (and behavioral) characteristics being utilized by law enforcement and the intelligence community. These include voice recognition, palmprints, wrist veins, iris recognition, gait analysis and even heartbeats.

Robots. Many law enforcement agencies are now using next-generation robotic cameras to deliver visual and audio surveillance of potential crime scenes that may be too dangerous or too hard for officers to reach.

Gunshot detection. Using mapping and electronic sensors, gunshot detection allows officers to respond immediately and accurately.

Data collection and crime analysis. Quick tracking and analyzing large amounts of data is important for law enforcement to do their jobs efficiently. With the help of cloud computing, police can access accurate statistics and real-time dashboards that monitor entire cities.

Language adviser L.I. Rusanova

UDC [811.111:351.74(100)](06)

Karina MALYNOVSKA

Kharkiv National University of Internal Affairs

THE USA AND UK INTERNET AS AN AID TO CRIME PREVENTION

There is a potentially very significant upside. Despite the challenges and potential vulnerabilities just outlined, it is possible to point to the Internet of Things as a whole as a new use case with regard to crime prevention and detection. When police started using distributed gunshot detection sensors called ShotSpotter in Camden, New Jersey, for example, they found that 38 percent of gunshots in one neighbourhood were not being reported or detected at all. This enabled the police to focus more resource on that area than previously had been the case. Visions of the future smart city envisage connected devices managing traffic flows, public lighting and other systems. If these systems were integrated with sensors and cameras across the cityscape they could have huge crime detection potential. One idea is to integrate

ShotSpotter with connected streetlight systems to help manage the response to firearms incidents. A recent commentary in Police Chief Magazine in the US painted the picture: ‘With a Safe Cities integrated technology approach, upon discharge of a firearm, the streetlights in the area (assuming it’s dark at the time) would immediately be brought to higher brightness. Video surveillance equipment in the area would be activated and turned in the direction of the gunfire and license plate readers would be activated to capture license plates in the area. The video would be captured and transmitted to the command and control facility and could then be relayed to the responding officers.’

More widely, the potential is that with enough connected devices deployed, law enforcement officers would be in a position to quickly know, in serious crime cases, where potential suspects were at the time of a crime, who they were with, and what they were doing. A Domain Awareness System already being used by the New York Police Department is already moving in this direction.

Cases are clearly now emerging where evidence gathered from internet connected devices is proving crucial in making arrests. In the UK, one case of multiple burglary was solved after BT wi-fi routers were examined in a row of four houses, each of which had been broken into in the middle of the day. The routers showed that the same mobile phone had connected to the free BT-FON service at each of the houses on the day the burglaries had taken place. The police were able to use that information to track down the perpetrator.

The blockchain technology might mean for policing and crime, the Internet of Things is a double-edged sword for law enforcement. The existence of a downside, however, just makes it all the more important that the opportunities of the Internet of Things are taken by the police.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Maksym MINAILO

Kharkiv National University of Internal Affairs

TECHNOLOGICAL INNOVATIONS IN POLICING AND CRIME PREVENTION

New technological innovations have been developed to prevent crime and to improve the performance of the police. Innovations in criminal justice technology can be divided into two broad categories: hard technology (hardware or materials) and soft technology (computer software, information systems). Hard technology innovations include new materials, devices, and equipment that can be used to either commit crime or prevent and control

crime. There are hard technologies intended to prevent crime – the ubiquitous CCTV cameras, metal detectors in schools, baggage screening at airports, bullet proof teller windows at banks, and security systems at homes and businesses. The use of personal protection devices (tasers, mace, lifeline/emergency call mechanisms) and ignition interlock systems with alcohol-sensor devices to prevent an individual from starting a car while intoxicated should also be noted. One can also identify hard technology innovations being used by police, including, new weapons, less than lethal force devices, new technology-enhanced patrol cars, and new police protective gear.

A wide range of new soft technology innovations have been developed in recent years and used as a crime prevention tool. Recent technology innovations include the latest generation of offender risk classification tools, the emergence of threat assessment protocols, bullying identification tools, software programs developed to prevent identity theft, new tools for monitoring the location and movement of at-risk populations, such as mentally ill offenders and sex offenders, and most recently, new assessment tools designed to identify individuals who are likely homicide offenders (or victims) within a specified timeframe.

Language adviser **L. I. Rusanova**

UDC [811.111:351.74(100)](06)

Anastasia MIROSHNICHENKO

Kharkiv National University of Internal Affairs

VIRTUAL CONFERENCE TECHNOLOGY AS NEW SKILLS FROM LITIGATORS

While video calls were not new when COVID hit, the widespread use of Microsoft Teams, Zoom, and other video conferencing technologies both within law firms and with clients has exploded with the pandemic forcing everyone to work from home. In addition to meetings, proceedings have moved online, with even high-profile trials taking place over Zoom. With courts adopting virtual hearing software like CaseLines, the trend of virtual hearings will no doubt outlast the pandemic and require new skills from litigators. Advocacy requires lawyers to be prepared, well-organized, have good materials, and to be civil and courteous — but, not surprisingly, there are additional factors to consider for virtual hearings and mediations.

A first consideration is to set “your intention for the virtual engagement, whether it’s an arbitration or mediation,” says Robin Dodokin, a lawyer, mediator and arbitrator at Dodokin Law & Conflict Resolution in Toronto.

“It’s very easy to feel like it’s just a conference call and be too casual,” she says; but “you have to get your head into the hearing, or mediation, ... even if you’re working on your kitchen counter.”

Special attention must be paid to interaction with other parties, “because they’re much more intimate” in a virtual environment, she says. If, for example, one is using two monitors and looking away from the camera at documents, “it can appear that you’re not paying attention.” And if your face is too close to the camera, “it’s not like a courtroom. Everything is magnified by the fact that we’re virtually in each other’s faces.”

The virtual proceedings may improve access to justice in civil matters in several ways: parties do not have to travel to the hearing and perhaps less time away from work, that it a time saving benefit; concerns about physical accessibility of court houses and buildings are not an issue; the technology is available to anyone with a smart device; some costs may be reduced as scheduling and case management matters can be dealt with virtually and quickly without a party or lawyer attending court; there may be some other cost reductions for virtual proceedings; for example, there are no room rentals costs or travel expense for witnesses; it has allowed dispute resolution to move forward effectively and safely during the pandemic.

Virtual proceedings will continue to be used past the pandemic and perhaps using a hybrid process of virtual and in-person. There will likely be more applications for virtual proceedings, owing to their advantages, and especially for international arbitration where there are parties and experts in countries around the world.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Lina MYTSYK

Kharkiv National University of Internal Affairs

HOW TOKYO POLICE USE DRONES

In 2015 the Phantom 2 drone carrying a tiny amount of radioactive sand was flown onto the roof of the Japanese prime minister’s office. The act was a protest against the country nuclear energy policy rather than a serious threat, but Japanese apparently saw it as something of a wake-up call. None was injured and a man was subsequently arrested in connection with the incident.

In order to combat such aerial threats in future, Tokyo Metropolitan Police Department has unveiled a net-wielding interceptor drone to be used to hunt down and snare rogue quadcopters.

A drone squad designed to locate and if necessary capture nuisance drones flown by members of the public, was launched by Tokyo Metropolitan Police Department. The police unit patrols important buildings such as the prime ministers office. If a suspicious drone is detected, the operator will be warned via loudspeakers on the ground. But if he or she fails to respond, police will launch drones equipped with nets to bring down the device.

Tokyo Police drones, complete with nets, might catch an unwanted airborne device in action. In Japan, it is illegal to pilot drones over certain areas such as airports and power plants, over roads, or above a height of 150m. Some cities such as Tokyo and Osaka have also outlawed their use in parks.

Regulations on drones came into force in Japan following an amendment to the country Aviation Act. Japan new net-carrying, drone-disabling drone is certainly an interesting way to police those areas where drones are forbidden.

Rules over drone use are being tightened up in several countries. In the US, for example, authorities have called for a drone register which would list device owners across the nation.

Language adviser L. S. Sazanova

UDC [811.111:351.74(100)](06)

Dmytro NAZARENKO

Kharkiv National University of Internal Affairs

PRE-CRIME TECHNOLOGY

The best way to fight crime is to keep it from happening in the first place, and technology is on the forefront of crime prevention. Again, AI tools and predictive analytics using big data are key to making connections that can stop crime before it starts, but law enforcement is using other tools in their work as well.

In Chicago, police officers are using technology called ShotSpotter, which triangulates information to determine the exact location of gunshots. Combining that information with license plate detection technology makes it easier for police to manage patrols in high-crime areas and investigate shootings. A gunshot detection system used in Chicago and other major cities that alerts police in real-time to the location of gunfire has launched in the south suburbs. Calumet City announced its deployment of ShotSpotter, a technology that uses strategically placed acoustic sensors to pinpoint gunfire and alert police within seconds of the precise location of that gunfire, the number of shooters and rounds fired, and the type of weapons being discharged. The California-based company, which has contracts with dozens

of cities across the country, does not guarantee its technology will reduce gun violence, but does bill its service as a crime-fighting tool that enhances safety for officers and aids in police investigations by facilitating a rapid response to shooting incidents that might not otherwise be reported to authorities.

Facial recognition technology is also proving instrumental to fighting crime. Law enforcement has used facial recognition at large events, for example, to identify individuals who are wanted for crimes by comparing their faces to a database of hundreds of thousands of known offenders. And at the border, U.S. Border Patrol agents are using sensor technology to evaluate physical and psychological behaviors to determine whether individuals are likely to be entering the country for nefarious purposes. The technology-driven revolution in policing is unfolding in big cities and small communities around the country, as more police departments purchase facial recognition software. Driven by artificial intelligence, facial recognition allows officers to submit images of people's faces, taken in the field or lifted from photos or video, and instantaneously compare them to photos in government databases — mugshots, jail booking records, driver's licenses.

All of these technologies are developed with the single purpose of preventing crime, and we're only seeing the tip of the iceberg when it comes to these tools..

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Tetiana NESKREBA

Kharkiv National University of Internal Affairs

BODY-WORN CAMERAS IN LAW ENFORCEMENT ACTIVITY

Supporters of body-worn cameras say they protect officers from false accusations, reduce agency liability and citizen complaints, and provide evidence for use in court. In recent years law enforcement agencies have been experimenting with and using body-worn video cameras. Unlike vehicle-mounted cameras, the body-worn cameras travel with the officer when he steps away from the patrol car. They can be attached to a shirt pocket, helmet, glasses or badge, and can serve to augment in-car video systems or provide an option to the expensive in-car systems that some departments cannot afford.

San Mateo (California), with a population of approximately 98,000, sits about 20 miles south of San Francisco, near Silicon Valley, which is home to numerous established and start-up high-tech companies. The police department has 100 sworn officers. The proximity to the technology enclave

has served the police department well, affording it the opportunity to serve as a testing ground for new technologies, such as a WiFi network that provides officers in the field with wireless broadband access to law enforcement databases.

In the past years the police department conducted five pilot tests of body-worn cameras, and decided not to use them though they are extremely important for policemen.

The police found that none of them were ready technology-wise for fulltime wearing. The cameras were not seeing what the policemen wanted them to see. It is not the perspective unless the camera is mounted on the officer's head, so for officers with a helmet it works well.

Vehicle camera systems have integrated automated license plate recognition technology. Future officer-worn cameras could also include it, as well as facial recognition software to scan the environment.

Language adviser L. S. Sazanova

UDC [811.111:351.74(100)](06)

Yulia NEZHURINA

Kharkiv National University of Internal Affairs

THE FUTURE PERSPECTIVES OF POLICING

New technologies, new methods, and new ideas have brought significant change to law enforcement. Police and law enforcement agencies across the country are driving the change, pioneering creative ideas, adapting to changing contexts, and incorporating insights from officers and community partners. The innovations that are shaping the future of law enforcement begin with emerging technologies that support new concepts of operations, enabling the interventions and relationships that keep society safe. Law enforcement is about keeping society safe. So it is no surprise that as society has changed, so too has law enforcement. New technologies, new methods, and new ideas have brought significant change to the profession. But at its core, law enforcement requires the same dedication to communities, the same sense of duty and sacrifice, and the same integrity it always has.

Today, the pace of technology is accelerating faster than ever. New devices and services seem to appear every day. We can now order anything, anywhere—from groceries to software to a ride from a complete stranger—using only a phone. We can reach anyone, or millions of people, in an instant. Our capacity to learn and to do good, and the capacity of some to do harm, is greater than ever. Technology is changing core aspects of how we interact as

a society, and as society changes, so too will the tools, techniques, and concepts the men and women of law enforcement use to keep us safe.

Innovation is not just about the latest gadget—it's about finding new ways to do things better. Innovations can take the form of new concepts, new methods, or new tools. But innovation tends to work best when all these forms come together to enable police and law enforcement agencies to have greater insight and impact than ever before. The innovations that are shaping the future of law enforcement begin with emerging technologies that support new concepts of operations, enabling the interventions, and relationships that keep society safe.

And though technologies, methods, and tools may continue to evolve, the core of law enforcement remains the same: tirelessly working to improve community engagement and public safety. Innovation is likely to bring greater insight and safety than ever before, but the same professionalism and discipline that brought law enforcement through the last century will continue to be keys to success in the next one.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Oleh OBERNIKHIN

Kharkiv National University of Internal Affairs

THE USE OF ROBOTICS BY THE POLICE OF THE UNITED STATES

Every day robotization penetrates into different spheres of life. Robots can get too dangerous, difficult or labor-intensive things done quickly. Robotics is in high demand by the US police. Drones, vision devices, sapper robots, patrol robots make the work of the police easier, make it safe for most police officers and allow to control more territories.

The New York City Police Department is using Digidog - robotic dogs from Boston Dynamics, although it is still in test mode. It is planned that they will be used in dangerous situations when there is a risk to the lives of police officers. Among the stated advantages of Digidog is the ability to see in the dark and assess how safe it is for a policeman to enter the premises. The police have already used Digidog in practice - for example, to free hostages. In addition to cameras, robots are equipped with speakers and microphone, so that officers can use them to negotiate with criminals. Police are confident that, thanks to Digidog, the number of injured and killed employees should decrease. Although there are fears that such robots, like any device, can be

hacked and used to harm - for example, unauthorized gathering of information about people. According to Michael Perry, vice president of business development at Boston Dynamics, the company takes tamper protection seriously, and the robots themselves were not conceived as hidden tools of mass surveillance as they are noisy and have a lot of blinking lights.

Knightscope makes futuristic autonomous robots designed to keep you safe while patrolling malls and other public places. The company also announced the possibility of face recognition. In case of detection of suspicious persons or criminals, a call to the hotline is made.

Modern technologies are gradually combining people and smart machines into one large social-apparatus network, so we need to acquire skills in managing and dealing with them.

Language adviser N.V. Krasnova

UDC [811.111:351.74(100)](06)

Anastasiia OSHCHEPKOVA

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN THE SERVICE OF US LAW ENFORCEMENT

Innovative technologies are radically new or improved technologies that significantly improve the conditions of production or act as a commodity. They usually have a reduced capital intensity, are characterized by greater environmental friendliness and lower energy needs.

In times of rapid technical development, innovative technologies are simply necessary in the police. They help fight crime and new categories of offenses. In this paper, we will discuss innovative technology in the service of law enforcement in the United States.

From drones and body-worn cameras to facial recognition software and artificial intelligence, here a list of the most important technologies that are equipping law enforcement with new capabilities for protection and service.

Facial recognition software

One of the most controversial new police technologies involves the use of facial recognition software. When this tool first entered the repertoire of law enforcement, many were concerned that it would be used unethically and could violate human rights. But fortunately, this has not been the case, and facial recognition has proven to be an effective investigative tool.

The purpose of facial recognition software is that it helps improve security in a number of cases. NYPD officers were able to locate and arrest a rape suspect within 24 hours of the attack using facial recognition software.

And because facial recognition is so promising, the U.S. Department of Homeland Security predicts it will be used 97 percent of the time by 2023.

Robots.

Many law enforcement agencies today use next-generation robotic cameras to visually and audibly monitor potential crime scenes that may be too dangerous or difficult for officers to access. Some of these devices, even "throwable" (up to 120 feet and capable of withstanding multiple falls from a height of 30 feet), run on an electric motor and are equipped with high-tech wheels that allow them to move, climb and explore even the hardest to reach wirelessly by a trained officer.

Automaker Ford has filed a patent for a self-driving police car equipped with artificial intelligence. These high-tech cruisers are designed to catch violators of traffic laws or impaired drivers by transmitting information to human officers or carrying an optional passenger officer who could make arrests.

Enhanced Body-Worn Cameras.

Video of police officers doing their job in difficult situations was rare, but today it is ubiquitous. With the help of cameras worn on the body, the ability of law enforcement officers and the public to get an idea of the police at the street level has increased.

In addition, thanks to constant improvements in technology, such cameras produce less bulky and more durable, and some body-worn cameras are designed to better integrate with automotive systems to provide synchronized video events from multiple points of view. Other advances include higher resolution, clearer sound, wider fields of vision and increased resistance to environmental conditions such as extreme cold.

A significant advance can also be considered "smart" holsters, which are designed to activate a body camera at any time when an officer pulls out his firearm. At least one manufacturer of body-worn police cameras has produced a camera capable of issuing an alarm when an officer falls. In the near future - cameras for wearing on the body, equipped with a function of face recognition.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Valeria OSTAPENKO

Kharkiv National University of Internal Affairs

THE FACE RECOGNITION (FR) TECHNOLOGY. BIOMETRICS

Police departments have long used biometrics, primarily fingerprints for identification. But now, many are using handheld scanners and facial recognition technology to improve speed and accuracy of identification.

According to PoliceOne, though these technologies are new, they are more common than we think: one-in-two American adult faces are in a law enforcement face recognition network. This 117-million face library housed by the FBI could assist officers with finding mission persons or comparing mugshots. However, there are some privacy concerns with the availability of this information. So law enforcement agencies have moved forward with this technology cautiously.

Chairman Chaffetz, Ranking Member Cummings, members of the committee says about the Federal Bureau of Investigation's (FBI) use of face recognition (FR) technology. The following FBI programs use FR technology for law enforcement purposes. They are: 1) the FBI's Next Generation Identification (NGI) System located at the FBI's Criminal Justice Information Services (CJIS) Division, and 2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit also located at the FBI CJIS Division.

1. NGI maintains a mugshot repository that is known as the Interstate Photo System (IPS). All mugshots are associated with tenprint fingerprints and a criminal history record. The NGI-IPS allows automated FR searches by authorized local, state, tribal, and federal law enforcement agencies. The law enforcement agency submits a "probe" photo that is obtained pursuant to an authorized law enforcement investigation, to be searched against the mugshot repository. The NGI-IPS returns a gallery of "candidate" photos of 2-50 individuals (default is 20). The law enforcement agencies then must manually review the candidate photos and perform further investigation to determine if any of the candidate photos are the same person as the probe photo. The NGI-IPS technology is only used as an investigative lead, and not as a means of positive identification. The NGI-IPS Policy Implementation Guide has been made available to authorized law enforcement users who receive candidate photos from the Next Generation Identification-Interstate Photo System. The policy advises that the photos are not being provided as positive identification and cannot serve as the sole basis for law enforcement action. In addition, the FBI has promulgated policies and procedures that place legal, policy, and security requirements on the law enforcement users of the NGI-IPS, including a prohibition against submitting probe photos that were obtained in violation of the First or Fourth Amendments. It is important to note that the FBI does not retain the probe photos; the probes are searched and deleted. Therefore, the NGI-IPS remains a repository solely of mugshots that are submitted voluntarily with fingerprints pursuant to arrest.

2. The FACE Services Unit provides investigative lead support to the FBI field offices, operational divisions, and legal attachés by comparing the face images of persons associated with open assessments² and active investigations³ against face images available in state and federal FR systems. In limited instances, the FACE Services Unit provides FR support for closed

FBI cases (e.g., missing and wanted persons) and may offer recognition support to federal partners. The FACE Services Unit only accepts “probe” photos that have been collected pursuant to applicable legal authorities as part of an authorized FBI investigation. Upon receipt of the photo(s), the FACE Services Unit searches them using FR software against databases authorized for use by the FBI, which results in a photo gallery of potential candidates. The FACE Services Unit performs manual comparisons of candidate photos against the probe photo(s) to determine a candidate’s value as an investigative lead. This service does NOT provide positive identification, but rather, an investigative lead and analysis to support that lead.

Using of automated FR technology to search probe images against a gallery, as described for the NGI, the FBI also utilizes automated FR as a way to organize or “triage” digital image files which have been obtained pursuant to an authorized law enforcement investigation.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Stanislav PAVLENKO

Kharkiv National University of Internal Affairs

DRONES IN THE LAW ENFORCEMENT SERVICE

The world is evolving at an incredible rate, with new technologies emerging every day to help both law enforcement and criminals. That is why the police must keep pace with the modern world and adopt the innovations that have succeeded in foreign countries.

Good example is Japan experience of using unmanned drones to detect and prevent illegal activities:

- drones with a net are used to catch drones that fly into unauthorized places carrying illegal objects or substances, as well as to intercept drones used for terrorist acts;

- observation of certain persons of persecution and video recording of their actions;

- patrolling the streets; a specialist who manages drones can monitor the actions of others from the air without leaving the office, and immediately record the offense;

- combating poaching; equipped with a thermographic camera, a drone at a distance of one kilometer can determine the exact location of persons, even at a night time;

- drones help in the search for missing people; having a high speed and aerial search, they are much more effective – one drone is enough to cover a huge area.

The effectiveness of drones in the law enforcement service is evident. In the USA the use of drones in the state during the year 2020 was the following:

93 law enforcement agencies from across the state Minnesota deployed drones 1,171 times – with an accumulative price tag of almost \$1 million. Almost half (506) were just for the purpose of “training officers.” Other uses included information collection based on reasonable suspicion of unspecified crimes (185), requests from other government agencies unrelated to law enforcement (41), road crash investigation (39), and preparation for and monitoring of public events (6 and 12, respectively).

Language adviser **L. I. Rusanova**

UDC [811.111:351.74(100)](06)

Victoria PIDGAINA

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES

An important element of the National Police is to deepen cooperation with active citizens. After all, effective protection of public order is impossible without the active participation of citizens interested in security. In today's world, certain innovative technologies are being developed for further work. One of them has already been implemented. For example, patrol police can drive on an electric scooter. The task of patrolmen is first of all preventive – in particular, to explain how to behave correctly on this type of transport. Inspectors will also be able to respond more quickly to calls.

Another example is the possibility of introducing official video recording or improving the recording of information provided. This method would make it easier to fight those who want to escape responsibility, as well as to record all the actions of the offender. It would be really effective that this process will be much faster.

An example of foreign inventors that would help in the fight against criminals – the Internet of Bodies. These are gadgets and applications that have the function of monitoring various displays the human body, but will also adjust and correct the indicators themselves. Devices will be connected to the brain, which will connect what is happening in real time with remote computers, which will receive data about work in the body. In addition to monitoring health, it can also increase cybersecurity by examining the human condition.

Approximately at least such principles of work have improved it. Therefore, I think it is possible to develop much more innovative technologies, but if we improved one of the proposed – it would be much better.

It is important to remember that innovative technologies not only improve and facilitate the work of the police, but also improve the fight against crime.

Language adviser N. L. Gorbach

UDC 351.74:001.895](100)(06)

Vladislav PILIPCHUK

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN THE SERVICE OF LAW AND ORDER

Ethics of digital technologies in the police. Extensive use of digital technologies in judicial and law enforcement activities is accompanied by great problem of ethics. The use of modern technologies by law enforcement agencies provides new opportunities to ensure the safety of citizens but poses a threat to human rights and freedoms.

Digital technologies in the work of the police. In order to effectively combat both traditional and cybercrime, law enforcement agencies should go one step ahead of offenders in using technical achievements. The advantage of the police is the collection and processing of a huge amount of data. At the same time, predictive policing comes to the force.

In the West, police services and judicial authorities are actively developing and using individual elements of digitalization and entire AI systems. According to Interpol and Europol, police officers in more than 70 countries use various types of predictive analytics in practice.

The main directions of the use of digital technologies in policing:

- improvement of police databases;
- predictive analytics to assess the likelihood of a crime in a specific territory;
- use of robots for patrolling;
- search and identification of missing people;
- quality control of police work;
- fight against corruption;

By order of the European Union, an international team of scientists developed and in 2013 launched the ePOOLICE system (early Pursuit against Organized crime using environmental scanning, the Law and Intelligence systems). To find signs of organized crime activity and assesses the risk of committing a crime, the system scans website pages, electronic correspondence, and police information.

Language adviser L. I. Rusanova

UDC [811.111:351.74(100)](06)

Vladislav POLTAVSKIY

Kharkiv National University of Internal Affairs

HOW BODY CAMERAS CAN HELP POLICE

As technology continues to evolve, law enforcement agencies are having to keep up. Agencies at all levels are investing in the latest and greatest technologies in order to better serve and protect their officers and communities.

Body cameras have been a great addition for many law enforcement agencies across the United States. While there are negative aspects of this technology that police officers need to be aware of, the body cameras have already proven to be useful in many instances across the country. The use of lethal force by police has been a big conversation over the past decade. With the never ending news cycle and virality of social media, these situations can quickly get out of hand before any facts have been brought to light. Body cameras are a technology that have helped the public get a front row seat to what police see and how they respond.

For example, in Cleveland, Ohio, four police officers faced trial regarding an instance where lethal force was used. Thanks to body camera footage, the public was able to hear and see the actions of those officers and decide if their actions were justified. In the wake of the murders of George Floyd, Breonna Taylor, and countless other Black lives at the hands of police, impacted families and community groups, police reform advocates, legislators, and even police departments have been calling for law enforcement agencies to adopt and expand body camera programs. This call is not new. Body cameras were proposed as a police accountability tool after the killings of Michael Brown and Eric Garner in 2014. They were called for after the police killing of Philando Castile in 2017, and they are being called for again today as police continue to brutalize Black lives and use excessive force on protesters advocating for racial justice.

Body cameras may serve more as a tool to monitor civilians and chill people's rights than to hold officers accountable. Because body cameras can roam through both public and private spaces, they capture enormous amounts of data about people beyond those interacting with the police officer wearing the camera.

Those who call for body cameras view the technology as a tool to better monitor officer conduct. Some advocates hope that the cameras will reduce misconduct and increase police accountability. In some cases, body camera footage has shed light on police misconduct that would not have been witnessed otherwise.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Rostislav PROKOPENKO

Kharkiv National University of Internal Affairs

SOME NEW POLICE TECHNOLOGY CURRENTLY IN USE

As the years came and went, so did plenty of other new technologies, from in-car laptops and body armor to new technology like smartphones and body-worn cameras. To put it simply, technology and policing go hand and hand. And that's a good thing, especially when this technology makes things safer for both officers and those whom they serve. As further technology inevitably develops, police have the opportunity to leverage it for the greater good in their departments and communities. What are some of the most effective tools police already use to promote public safety?

Police drones. Used by the military for many years, unmanned aerial vehicles, or drones are becoming increasingly common in law enforcement. Many departments use them for surveillance or collecting evidence. Others use them for taking pictures of crash scenes and even controlling crowds. Drones are also helpful for other areas of law enforcement, as they can monitor correctional facilities and track escapees.

GPS. GPS has also been used by police departments for many years. Officers have most frequently used it to track criminals, but more recently, GPS has helped in officer safety monitoring. New developments in GPS technology is giving officers more information and detail than ever before, ensuring safety and efficiency on the field.

Officer tracking. GPS allows for better coordination and tracking of where officers and vehicles are. This can help departments dispatch more efficiently to incidents. It also allows for more precise location information for calls, and for more safer, faster routing of officers to those incidents..

Vehicle pursuit darts. Pursuit-related crashes result in more than 55,000 injuries every year. What if you could track vehicles in pursuit situations from a distance, keeping your officers and other drivers safe on the road? They aren't too common yet, but vehicle pursuit darts, like a real-time, physical GPS, do just that. A small, foam dart that can be shot at a vehicle, they enable officers to safely tag, track, and apprehend dangerous individuals.

Gunshot detection. Gunshot detection isn't in use by many departments, but it can be a very helpful way to monitor for gunshots in specific areas. Using mapping and electronic sensors, gunshot detection allows officers to respond immediately and accurately. Some departments use gunshot detection to fill in gaps, identifying shots fired that don't get called in. "We found rates of random gunfire that were astounding to us," Nassau County deputy commissioner William Flanagan tells ComputerWorld. "What was more

bothersome was that we were not getting calls about it.” Clearly, this technology is helpful, but it’s also expensive. If your area has high occurrences of gunfire, it may be worth it. Areas with scarce witnesses might also find gunshot detection to be a wise investment.

However, it’s helpful to know that technology always evolves and likely never be short of opportunities to implement new systems that could add safety and efficiency to every department.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Daryna PRYKHIDKO

Kharkiv National University of Internal Affairs

LATEST TECHNOLOGIES FOR TERRORIST THREATS PREVENTIONS

Due to technological advances the globe is flooded with equipment which both terrorists and those who fight them are interested in. Terrorists might increasingly use modern technology with bad intentions. Science and technology specific to countering terrorism includes the means of ensuring premature detonation of explosives or of inhibiting the triggering of explosives. Most science and technology counter-terrorism tools are highly useful for public health, law enforcement, or intelligence purposes.

Security technologies allow for real-time identification, location and scenario planning of terrorist intentions by forecasting likely risks. They also make it possible to target the mobility, communications and financial and banking transactions of terrorists. Biometrics is one of these technologies with numerous applications, including DNA, iris and retinal scans, facial and even emotional recognition.

Surveillance consists of the observation, collection, recording and processing of information relating to individual movements, itineraries, behaviours and communications to attribute a probable degree of risk.

Technology also contributes to identifying and locating elusive terrorists with predictive artificial intelligence. Based on data mining (mining data from large interconnected databases), predictive technologies use mathematical models.

Drones are served for video surveillance and remote elimination of terrorists, as well as a means of reconnaissance of routes and attack sites, real-time monitoring of activities or as improvised explosive devices (flying, sea or land).

Language adviser L. S. Sazanova

UDC [811.111:351.74(100)](06)

Vladislav REPALOV

Kharkiv National University of Internal Affairs

INNOVATION AND SCIENCE AS THE BASIS FOR IMPROVING LAW ENFORCEMENT

Today, our country continues to form a modern, effective, high-quality and strong mechanism of state bodies. A special role in this mechanism is played by law enforcement agencies and, in particular, the police, which are responsible for ensuring the rights and freedoms of citizens and protecting the established order, preventing unlawful encroachments.

Despite the changes, the system of law enforcement agencies remains insufficiently effective and closed from society. To change this situation, police officers need to constantly develop and improve their professional skills both physically and spiritually.

There are different ways to develop professional police qualities, for example:

- participation in scientific seminars and trainings;
- communicate with citizens to increase the level of public confidence.
- Participation in various projects aimed at developing the personal qualities of a police officer.
- communication with foreign colleagues and learning from experience;
- International Law Enforcement Partnership

An example of such a partnership to improve law enforcement is The National Police Foundation in the United States, a national, nonpartisan, non-profit organization dedicated to improving policing through innovation and science.

Now the organization cooperates with hundreds of police institutions throughout Ukraine, as well as at the international level, providing research and translation, training, technical assistance and the introduction of modern technologies. The Foundation is a leader in the safety and well-being of officers, the protection of public services, open data, investigations and security technologies. The main objective of the Foundation is to contribute to improving the quality of police services in order to benefit the staff and communities they will serve, as well as to reduce crime.

Language adviser G. S. Babak

UDC 351.74:001.895](100)(06)

Daria RIABTSEVA

Kharkiv National University of Internal Affairs

ROBOTS IN THE WORK OF LAW ENFORCEMENT AGENCIES

Law enforcement professionals are using global positioning technology to perform different tasks, confirming the presence of suspects at a crime scene included. Some robots can even perform the same rigorous tasks as officers have to carry out, enabling them to focus on more important activities

Many law enforcement agencies are now using next-generation robotic cameras to deliver visual and audio surveillance of potential crime scenes that may be too dangerous or too hard for officers to reach.

Some of these devices are even “throwable” (up to 120 feet and capable of withstanding repeated 30-foot drops) – powered by an electric motor and equipped with high-tech wheels that enable them to move, climb and explore even the most challenging spaces while being operated wirelessly by a trained officer.

Automaker Ford has filed a patent for a self-driving police car equipped with artificial intelligence. These high-tech cruisers are designed to catch violators of traffic laws or impaired drivers by transmitting information to human officers or carrying an optional passenger officer.

Additional applications for using robots in police work, now and on the near horizon, include:

- Ever-expanding capabilities for robots to gather surveillance information, take police reports and provide communications in settings where human officers’ safety would be compromised.

- China’s ongoing development of an “AnBot” robot to patrol banks, airports and schools.

- Patrolling tourist attractions with a touchscreen-equipped robot officer, as is now on duty in Dubai.

Language adviser L. I. Rusanova

UDC [811.111:351.74(100)](06)

Yulia ROGOZHINA

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN POLICE

New technologies, new methods, and new ideas have brought significant change to law enforcement. Law enforcement is about keeping society safe. So it is no surprise that as society has changed, so too has law enforcement.

New technologies, new methods, and new ideas have brought significant change to the profession. But at its core, law enforcement requires the same dedication to communities, the same sense of duty and sacrifice, and the same integrity it always has.

Consider the five best innovations in policing that shape the future :

1. Combining emerging technologies to gain greater awareness, faster

Every investigative journey begins with collecting facts about the world. Traditionally, this work has been tough. It could mean relying on a officer's memory of a license plate to look out for, or long hours searching for the right pieces of information. It often means being there, to see, to hear, and to deter—and no department can be everywhere. However, new technologies, like the Internet of Things (IoT) and smart sensors, can be there when needed.

Smart sensors can be used to compile many different types of information to help officers do their jobs faster and more effectively. New capabilities can log locations, listen for gunshots, stream video, flag license plates, scan databases, and go on virtual patrol, allowing officers unprecedented awareness in their environments.

2. Harnessing digital technologies to improve officer and citizen safety

Internet of Things and distributed sensing are about leveraging new technology to gather information about the world, and point in the right direction. But what should officers do on the scene? New technologies and practices are developing that can help guide action in the world. Advances in areas such as 5G communication, electronics miniaturization, and augmented reality allow people to see, hear, and act in ways that were previously impossible.

3. Leveraging mountains of data to prevent crime

We live in a world awash in data. And as many departments deploy technology solutions like augmented reality, body cameras, license plate readers, and smart sensors, they will likely generate more data each day than in their entire analog histories. The success of future law enforcement strategies rests on being able to quickly and efficiently harness these immense volumes of data to support investigations and enforcement actions. But these mountains of data are too vast for any human to comb through, even if they dedicated an entire lifetime to searching.

To gain real insight, artificial intelligence (AI) and machine learning will be key to future investigations. For example, each year more than eight million tips on the location of missing children must be analyzed by a team of just 25 investigators. AI is being deployed to help those investigators sift through the data and find the most likely leads to identify exploited children and reunite them with loved ones. AI is already demonstrating its value around the world by helping police in England analyze CCTV video, officers in India find 3,000 missing persons in just four days, and the Dutch to find promising leads in cold cases.

4. Rigorously testing what works and scaling key insights

AI and machine learning can help find the clues to target a patrol or forward an investigation, using simple rule sets to test new hypotheses, identify what works, and scale successes. A similar approach—evidence-based policing—can also be applied to the methods of police work itself. Evidence-based policing includes using advanced forensic techniques to extract more information from the same amount of evidence, but it also goes beyond this to examine the heart of police activities.

Evidence-based policing can analyze data about the outcomes of police interactions to help find the most effective methods and tools while minimizing the use of tactics that tend to make situations worse.¹⁰ In an era when many police officers are being asked to do more and more with fewer and fewer resources, evidence-based policing seeks to pair them with outside assistance, such as academic researchers or computer programmers, to help focus their efforts on the most effective police work.

5. Forging stronger local networks to improve public safety

The mission of law enforcement is the safety of the community, and a strong relationship with the community is critical to the success of every law enforcement organization. Building close ties within the community is about traditional police outreach and local involvement, but it's also about leveraging tools to help people communicate their needs and their risks directly. New technologies can help police develop their ties to the community, by enabling officers to be more aware of and responsive to the needs of their constituents.

Change is inevitable, but law enforcement agencies can take proactive steps to prepare for the future. Along with these future trends, changing demographics are shifting what the officer of the future will look like and how they will spend their day. Law enforcement leadership must recognize these changes not only to recruit the right personnel, but also to manage them effectively in a world shifting from bricks and mortar to bits and bytes.

And though technologies, methods, and tools may continue to evolve, the core of law enforcement remains the same: tirelessly working to improve community engagement and public safety.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Valeriia ROMANOVA

Kharkiv National University of Internal Affairs

AN IMPORTANCE OF DATA COLLECTION AND INFORMATION GATHERING

Laws should direct the appropriate state agencies to collect quantitative data relating to “honour”-based violence. Quantitative data is obtained by measuring indicators of prevalence, government response, and program performance. This data can be obtained by state statistics offices by utilizing surveys administered to the general population and by obtaining data from relevant administrative sources, such as hospital and police records. The Manual for the Development of a System of Criminal Justice Statistics includes a section on victimization surveys, which take into account the fact that many crimes may go unreported and that victimization and self-reporting surveys will help reveal these crimes. This is particularly relevant to “honour” crimes, as many experts estimate that the actual number of such crimes far exceeds the number of reported cases. Drafters should ensure that laws require the gathering and dissemination of statistics related to “honour” crimes and establish a database to track such information. Authorities should collect data on the following indicators: the forms of “honour”-based violence, incidence, causes and risk factors, the linkages between economic deprivation and exploitation and “honour”-based violence, short-, medium-, and long-term consequences, effects on population sub-groups of women and girls, prosecution rates, convictions, penalties, the relationships between the victim and perpetrator(s), victimization patterns including repeat or multiple victimization, ethnicity, age, sex, disability, religion, and the use of weapons or dangerous substances.

Laws should allocate adequate public funding for qualitative studies to better understand the causes, dynamics and consequences of “honour” and “honour” crimes in the applicable country. Qualitative data goes beyond the scope of statistics to provide a deeper, more nuanced understanding of the issue. For example, the Council of Europe Convention on preventing and combating violence against women and domestic violence calls on states parties to support research on all forms of violence against women “in order to study its root causes and effects, incidences and conviction rates” (Art. 11(1)). Monitors should also assess existing legislation, policies and programmes for the prevention of violence against women, the prosecution of violent offenders, and the protection of survivors. They should then analyze how effective these laws, protocols, and programs are in attaining victim safety and offender accountability and preventing violence against women.

The UN Office of the High Commission for Human Rights has issued a Training Manual on Human Rights Monitoring and a Trainer's Guide, which provides guidelines for human rights monitoring.

While all of the principles set forth in the UN Training Manual are essential, the principle of doing no harm and maintaining confidentiality is of the utmost importance to protect victims and prevent further victimization or harm. The fact-finder's principle duty is to the victim or potential victims of human rights violations, and at a minimum, the fact-finder must refrain from actions or omissions that would endanger their safety.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Bogdan ROSHENKO

Kharkiv National University of Internal Affairs

THE IMPORTANCE OF RELEVANT DATA COLLECTION FOR CRIME-FIGHTING

Data literacy – the ability to derive meaningful information from data – should be the goal of every agency. Many departments are downloading information from CAD dispatch systems, uploading information from police officer's vehicle-mounted computers, and sending information wirelessly using e-citation machines, all without understanding why and how the data is collected. Understanding the “why” behind data collection will help encourage how the data is collected. The goal should never be to collect random data just to add to the pool of previously collected data – random collections of data will lead to an ocean of unusable data like what we have now. The goal should always be to collect data for a specific purpose: crime-fighting. Once the data is collected with a purpose, it is now the job of the crime analysts and detectives to convert that data into information, then turn that information into insight.

Police agencies need more relevant data and less garbage that analysts and detectives can quickly convert into usable information. The fact is there is a TON of data out there. Law enforcement needs smart tools to help deliver the right/relevant information. Luckily, correcting irrelevant data collection habits is as easy as 1,2,3:

1. Numbers pose an interesting problem for data collectors because they can be easily transposed. The numbers on VINs, license plates, serial numbers and addresses should be verified before recording it into any software.

2. Individuals: Accurate data collection on people can also pose a problem. Many people share the same first and last name so collecting

distinguishing characteristics is just as important as names. In Arizona, for example, 43 people share my first and last name; 4 share the same first, middle and last name; and 1 is a released violent felon from another state. Pay close attention to personal identifying information (PPI) including complete legal name, accurate social security number, visible tattoos and tattoo location, and race.

3. Associates and friends: Document friends and associates and I promise your analyst will thank you later! Always ask the passengers of traffic stops and friends of your suspect for their PII, too. Just remember in most states, passengers of traffic stops do not have to talk with you unless you have a violation on that person, but at least you can try.

As you could see, the more accurate the information, the easier it will be to turn that information into insight. Big data needs to be made small to be effective. The best way to start to shrink data is by understanding the why behind the collection, recording accurate information and using analyzing software to turn data into insight so you are not left floating in an ocean of undrinkable data mumbling to yourself, “Data, data everywhere but not a drop to drink!”

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Artur ROZUM

Kharkiv National University of Internal Affairs

HOW TO IMPROVE POLICE WORK THROUGH INNOVATION AND SCIENCE

With comprehensive electronic databases now in place to more effectively use DNA and other biometric data in law enforcement, even the use of fingerprints to identify suspects has gone high-tech.

For example, CNBC (Consumer News and Business Channel) report explains how police in London can now use a mobile INK (Identity Not Known) biometrics device to scan a suspect's fingerprints and in many cases reveal their identity within 60 seconds.

An officer's patrol car is like a mobile command center, meaning there are numerous computers and tools that an officer can use while on the road.

One of the latest innovations being incorporated into police cars is a new voice command technology that empowers officers to control many functions in their vehicle while driving and performing other patrol duties.

The capabilities of these voice systems vary from vehicle to vehicle, but most can handle commands to run a license plate or turn on a siren. The more advanced and most promising capability of voice command technology in

police cars will make filing reports much easier – officers can dictate their notes which are then logged directly into their agency's RMS (Remote Manipulated System).

Many law enforcement agencies are now using next-generation robotic cameras to deliver visual and audio surveillance of potential crime scenes that may be too dangerous or too hard for officers to reach.

Some of these devices are even “throwable” (up to 120 feet and capable of withstanding repeated 30-foot drops).

Language adviser L. S. Sazanova

UDC 351.74:001.895](100)(06)

Andrii SEMCHUK

Kharkiv National University of Internal Affairs

USE OF PROGRAMS FOR ANALYSIS OF NETWORK PROTOCOLS

In the era of high information technology, when everything is developing at a rapid pace, criminals are increasingly using the Internet to carry out their crimes. However, law enforcement agencies do not stand still and use more advanced methods for operational and investigative activities.

A variation of these methods is the use of software tools for scanning and analyzing traffic for computer networks. These methods are actively used in the cyber police units of different European countries.

One of them is Wireshark. Wireshark is an open-source network protocol analysis software program started by Gerald Combs in 1998. A global organization of network specialists and software developers support Wireshark as it is absolutely safe to use. There isn't a better way to learn networking than to look at the traffic under the Wireshark microscope. There are questions about the legality of Wireshark since it is a powerful packet sniffer. Because you should only use Wireshark on networks where you have permission to inspect network packets.

Today wireless network technology allows persons with a compatible wireless card to capture packets of data destined for another computer, due to the fact that radio waves are the media through which data sent wirelessly travels. Therefore, a police officer can theoretically attempt to gather digital evidence against a suspect by traveling to the immediate vicinity of the suspect, using his or her computer wireless networking card to capture any packets in the area, then analyzing the packets to try to glean information that could be useful for an investigation.

Language adviser L. I. Rusanova

UDC [811.111:351.74(100)](06)

Ruslan SHEPELENKO

Kharkiv National University of Internal Affairs

INTELLETUAL PROPERTY THEFT AND HOW TO MANAGE YOUR IP TO STAY SAFE

More commonly known as piracy, the Internet abounds with books, music, movies, and more that have been illegally obtained and made available for free download. Despite what some people say, piracy is not a victimless crime. Not only do artists and creators lose out, but many illegal downloads also contain hidden malware that can destroy your computer. With the online space becoming more crowded, cloud computing becoming the mainstream, and just about everything located on the internet, stealing intellectual property has become easier than ever before.

Intellectual property can be movies, music, content on the web, software and more. You can think of IP as creations and not necessarily physical products. But, this doesn't mean that the damage is less than other types of theft. IP theft damage is estimated at hundreds of billions of dollars a year according to the Commission of the Theft of American Intellectual Property. Intellectual property theft is one someone steals an idea, creative expression, or invention from an individual or a company. IP theft can refer to someone stealing patents, copyrights, trademarks, or trade secrets. This includes names, logos, symbols, inventions, client lists, and more. Intellectual property theft cases are exceptionally common and require smart intellectual property management software in order to be avoided. Most intellectual property theft cases are considered federal cases (therefore federal crimes). Companies or individuals that can identify who stole their IP can bring them to court and in some cases, serious penalties can be given to the criminals. These include fines, imprisonment, civil charges, suspension of licenses, etc.

If someone has stolen your intellectual property, there are several steps you can take to remedy the situation. In most cases, the first thing to do is to ask the person or company that has stolen from you to stop using your IP. After all, IP theft is a crime so the person may agree to stop using the IP immediately. In some cases, IP theft is non-intentional (for example if a license expired). In more complicated intellectual property theft cases, you may have to take legal action. Usually, this begins by having an attorney send a letter about the alleged crimes. In many cases, the issue stops here. If it doesn't you may have to move on to an actual lawsuit.

In today's post-COVID world, cybersecurity threats and attacks are rising rapidly. This is the time that companies need to make sure that their IP is protected against third parties and those looking to hold IP ransom for hefty

fees. 2022 has been called by some the year of cybersecurity. As workers move to work-from-home models, VPN vulnerabilities are being exploited and companies cannot keep up with the security breaches that they are encountering. With that, ransomware attacks are continuing to increase, with enterprises paying out large sums just to get back to work as normal. Using intellectual property management software helps companies keep track of their IP (specifically software, licenses, etc.).

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Tatyana SHEPILOVA

Kharkiv National University of Internal Affairs

THE MOST PERTINENT REASONS FOR THE RECENT SHIFT IN THE LEGAL INDUSTRY

Innovation in law is no longer a trend or mere hype, but a tangible and urgent need. Law firms and corporate counsels are at a crossroads, with changes to the legal landscape in the last few decades preventing them from carrying on business as usual. Lawyers have a choice: ride this wave, or risk missing out on the chance to play in the big league of tomorrow's law industry.

Across Europe, significant changes in the civil and commercial sphere are forcing law firms and in-house counsel to transform and adapt to this new ecosystem. Large and prominent law firms are still at the top of the pyramid. However, some relatively new firms and legal tech companies are taking on an increasingly prominent role in the market. For both incumbents and new agents, innovation matters. If lawyers across the board are to remain relevant in this emerging landscape, they must have a firm understanding of why innovation in law matters—an understanding that goes far beyond an appreciation of the hype. Below are some of the most pertinent reasons for the recent shift in the legal industry.

Legal work of the past no longer cuts it. Whether we're talking about clients of a law firm or the internal clients of an enterprise, neither will continue to accept work on the same basis as they did ten years ago. It is not only a question of billable hours, but efficiency. No client is interested in wading through the fog of fees, coming out the other side with a hefty bill and a headache. Nowadays, dozens of legal providers offer the same expertise and quality of work, but those that will survive are able to provide certainty of fees to their clients.

Young lawyers have completely different goals. Clients are vital, but talent is of the essence in the legal sector. The next generation of lawyers are the ones who will help us ride the digital tsunami. No other generation in history is so close to technology. As digital natives, they are best placed to help firms adapt, evolve, and stay relevant now and in the future.

Technology has transformed internal processes. Lawyers used to identify themselves as artisans or craftsmen. Those who still think this way, will be pushed out of the legal market. Law is no longer an art - it's a science.

New agents are taking a piece of the pie. The legal market is no longer the exclusive domain of lawyers. New law firms combine both legal and technical staff to better understand clients' needs and offer the most appropriate solution.

Let's not forget that the industry is full of opportunities. Although the legal market is extremely mature, we have seen how the most disruptive law firms and general counsel operate and deploy new products and services every year. No matter the location or the area of law, the legal industry is eager for new content and innovation.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Nikita SHEVCHENKO

Kharkiv National University of Internal Affairs

DATA PROTECTION IN THE SERVICE OF POLICE

All data or information that relates to an identifiable individual that business stores or handles needs to be properly protected. From financial information and payment details to contact information for the staff.

What data needs to be protected?

Key pieces of information that are commonly stored by businesses, that is employee records, customer details, loyalty schemes, transactions, or data collection, need to be protected. It is necessary to prevent all data from being misused by third parties for fraud, such as phishing scams and identity theft.

Common data that business might store, include names, addresses, Emails, telephone numbers, bank and credit card details, health information.

This data contains sensitive information that could relate to the current staff and their partners or next of kin; shareholders, business partners and clients; customers and other members of the public.

Protecting all this information, in accordance with the Data Protection Act, requires businesses to adhere to specific principles.

Law. The Data Protection Act contains a set of principles that organizations, government and businesses have to adhere to in order to keep someone's data accurate, safe, secure and lawful.

These principles ensure data is:

- only used in specifically stated ways.
- not stored for longer than necessary.
- used only in relevant ways.
- kept safe and secure.
- used only within the confines of the law.
- not transferred out of the European Economic Area.
- stored following people's data protection rights.

This comes into practice in business particularly when you recruit staff, amend staff records, market your products or services, or use CCTV.

Language adviser: L. I. Rusanova

UDC 351.74:001.895](100)(06)

Karyna STARCHENKO

Kharkiv National University of Internal Affairs

WILL POLICEMEN BE REPLACED BY ROBOTS?

Police Robots are designed to allow access to situations that are inaccessible or dangerous for first responders. They can manipulate objects as well as gather data through a variety of technologies. These robots are suitable for a range of environments with varying data and communication capabilities. New security robots are fulfilling human role: the beat cop. They patrol neighborhoods at a walking pace, looking for crime.

Using robots in police work, now and on the near horizon, include: ever-expanding capabilities for robots to gather surveillance information, take police reports and provide communications in settings where human officers' safety would be compromised.

An advanced security technology company Knightscope based in Silicon Valley (the United States of America) builds fully autonomous security robots that deter, detect and report. It has sold more than 50 of its artificial intelligence-powered, autonomous security robots to more than 20 clients. Their conical, five-foot robots feature four cameras and can scan license plates and pick up on individual cell phones' MAC addresses. While they don't look like a classic police officer with dress blues, they patrol the block at walking speed to keep neighborhoods safe.

Their effectiveness has been difficult to prove so far, but behaviorally, they bring to mind the issue of humanoid robots.

Artificially intelligent robots are an increasingly common crime-fighting tool for police and other law enforcement personnel across the world, but they won't replace humans anytime soon because this job is ranked 167 out of 702 and a higher ranking (i.e., a lower number) means the job is less likely to be replaced.

Language adviser L. S. Sazanova

UDC [811.111:351.74(100)](06)

Daria SVISTUN

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN THE POLICE

The COVID-19 pandemic has accelerated the need to bring new tech solutions to fulfill unanticipated needs like policing during a pandemic with social distancing measures in place. The capabilities that these technologies have brought to policing during the age of COVID-19 will continue to evolve and stay relevant for years to come.

In the context of the pandemic, there are some innovations in the legislation governing the National Police that can help counter the pandemic. National police officers should be involved in ensuring quarantine restrictions - preventing the spread of rumors and fakes that can cause panic, monitor the activities of outlets and transport, monitor the implementation of the "mask regime" in public places. At the same time, the police themselves must be protected from the risk of infection.

In the context of the fact that the pandemic is global - consider the main challenges facing law enforcement agencies not only in Ukraine but also around the world.

CHALLENGE 1: SCHEDULING, STAFFING AND BUDGETING FOR UNKNOWNNS

Staffing, scheduling and budgeting have been a challenge for many law enforcement agencies, even before COVID-19.

Not only do agencies need to look for ways to minimize possible exposure, but also plan for the likelihood of an officer becoming infected. Some of those officers may need to self-quarantine or take sick time off. The reality that the virus can have serious and even fatal consequences means that agencies also need to plan for long-term disability or death (and the cost and personnel ramifications from those possibilities).

CHALLENGE 2: SITUATIONAL AWARENESS NOW INCLUDES ASSESSING COVID-19 RISKS TO CITIZENS AND FIRST RESPONDERS

Since first responders by the very nature of their jobs are required to be out in public, another challenge becomes how to keep them safe during a pandemic.

The instant chat function is an effective tool to communicate in real time with sick or masked patients as well as deaf and hard of hearing. And the platform's location services are based on the caller's device location, allowing responders to pinpoint location even within a building complex or densely populated area.

CHALLENGE 3: CONTROLLING THE VIRUS AND MEETING NEEDS IN GROUP ENVIRONMENTS THROUGH DATA COLLECTION

Because of shared environments and close quarters, correctional and detention facilities have the potential to be hot beds for COVID-19 cases. According to the Centers for Disease Control, prompt identification of persons with COVID-19 and consistent application of prevention measures within correctional and detention facilities are critical to protecting incarcerated or detained persons, staff members, and the communities to which they return.

Juware has created a Pandemic Dashboard that makes it easier for correctional facilities to track cases on a daily basis in order to understand the impact on facilities, inmates and staff.

CHALLENGE 4: MANAGING PROBATION AND PAROLE WHILE MINIMIZING IN-PERSON CONTACT

Incarcerated individuals returning into the community and those on probation are already at risk of slipping back into the situations that got them in trouble in the first place. One missed check-in due to transportation or other issues can have dire consequences that set them back. The COVID pandemic and the associated disruptions make the challenge even greater and have forced agencies to take a different look at ways they use technology to manage offender populations.

CHALLENGE 5: REDUCING THE NEED FOR FACE-TO-FACE ENCOUNTERS FOR NON-EMERGENCY CALLS

Police departments are already stretched thin, and the COVID-19 pandemic has potentially diminished the ranks even further. To reduce the possibility of exposure, law enforcement agencies are having to prioritize the types of calls for service that will result in an officer being dispatched to the incident scene.

Since citizens are increasingly using apps like FaceTime and Google Hangouts to interact with each other over video chat. Many law enforcement officers were already using 10-21 Police Phone to interact with citizens over the phone without revealing their private phone number. When COVID hit, many of those officers found the app also helped them reduce the need for

face-to-face encounters for routine police work that could be handled by phone.

While these technologies have been created or enhanced to help law enforcement adapt to changing conditions due to the COVID-19 pandemic, many of these challenges existed before the pandemic and will continue to exist as the world adjusts to a new normal.

Benefits like enhanced situational awareness, improved location accuracy, greater access and sharing of data and streamlined processes will lead to greater safety for law enforcement officers and the people they serve. The solutions born of this crisis may continue to be refined – but doubtless they are here to stay.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Mykyta TALAN

Kharkiv National University of Internal Affairs

OPEN SOURCE INTELLIGENCE CRIME INVESTIGATION

Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources (overt and publicly available sources) to produce actionable intelligence. OSINT is primarily used in national security, law enforcement, and business intelligence functions and is of value to analysts who use non-sensitive intelligence in answering classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines.

OSINT sources can be divided up into six different categories of information flow:

Media, print newspapers, magazines, radio, and television from across and between countries.

Internet, online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, etc.). This source also outpaces a variety of other sources due to its timeliness and ease of access.

Public government data, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.

Professional and academic publications, information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.

Commercial data, commercial imagery, financial and industrial assessments, and databases.

Grey literature, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.

OSINT is distinguished from research in that it applies the process of intelligence to create tailored knowledge supportive of a specific decision by a specific individual or group.

OSINT is defined by both the U.S. Director of National Intelligence and the U.S. Department of Defense (DoD), as intelligence "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." As defined by NATO, OSINT is intelligence "derived from publicly available information, as well as other unclassified information that has limited public distribution or access.

Open Source Intelligence (OSINT) is security-related information collected from freely available open sources (e.g. social and professional networks, news, websites). Appropriate analysis tools are used to gain usable insights from the various pieces of information.

These sources can be free or subscription-based, online or offline.

Open Source Intelligence is not limited to the Internet, but can also use freely accessible mass media as a source, such as magazines, daily newspapers, radio and television.

OSINT can be used in the area of cyber security, for example for hacking, social engineering, penetration testing and security analysis. For this reason, it makes sense for organizations to collect and evaluate OSINT information and react accordingly.

Potential sources are: forums and blogs, social and professional networks, Databases with software errors (Vulnerability Data Bases), Deep and Dark Web, job advertisements, Web pages, other internet sources.

Benefits of Open Source Intelligence. The costs for obtaining information are low due to the increasing degree of digitization and the large amount of freely available information on the Internet.

The procurement of information can be easily implemented using automated analysis tools.

The risk of discovery is low because the information is accessed via public infrastructure and technology.

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Oleksandr TESLENKO

Kharkiv National University of Internal Affairs

PHISHING ATTACK AS A TYPE OF CIBERCRIME

Phishing is when criminals send fraudulent emails pretending to be from legitimate businesses, in an attempt to collect sensitive, personal information. Often, any links in the email will redirect to a website owned by the scammer, so always be careful about what information you give out on the Internet.

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data. An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

The email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates. For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate. In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, as previously shown, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.

How to prevent phishing? Phishing attack protection requires steps be taken by both users and enterprises. For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its true identity. These can

include spelling mistakes or changes to domain names. Users should also stop and think about why they're even receiving such an email.

Language adviser V. V. Kochyna

UDC 351.74:001.895](100)(06)

Elvira TKACHENKO

Kharkiv National University of Internal Affairs

ADVANCED MODERN TECHNOLOGY HELPS POLICE FIGHT CRIME

Police cruisers have come a long way since the first police car hit the streets of Akron, Ohio, in 1899 (with a gong for a siren and Ace fight crime cell in the back for prisoners).

Innovation in modern police cruisers (and those of the future) has brought about such upgrades as fingertip access to Wi-Fi connected laptops, tablets, and in-dash computers, giving officers the benefit of instant access to vital information, communication systems, and more.

Enhanced dash cam capabilities are highly useful for surveillance and information gathering, as well as for evidentiary and accountability purposes. Next-generation officer safety features (for example, armor-piercing bulletproof doors) are also being incorporated into some police vehicles, and semi-autonomous operational capabilities are not far down the road.

The same technology that enables toll collectors to automatically scan and collect the registration numbers and letters on the license plate to charge you a fee is now being used by police for a variety of law enforcement purposes, from identifying stolen cars to catching up with people who have active warrants or monitoring “Amber Alerts.” However, the technology law enforcement uses for ALPR (Automatic License Plate Recognition) has taken another innovative step forward.

The latest in ALPR technology combines optical recognition technology with AI (Artificial Intelligence), allowing law enforcement to reliably and consistently identify license plates.

Before the enhanced AI capability, some ALPR cameras provided low-resolution and blurry images, making proper identification difficult. With AI, ALPR cameras can identify the make, model and color of cars even in low light and poor weather, distinguish individual characters on license plates, learn new plates as they appear and expand its database to include updated and unfamiliar designs.

Language adviser L. S. Sazanova

UDC [811.111:351.74(100)](06)

Yulia TUYAHOVA

Kharkiv National University of Internal Affairs

OBSTACLES IN ORGANIZATIONAL COMMUNICATIONS

Obstacles that arise in the field of communications are divided into obstacles in communication between individuals and in organizational communications.

Barriers to interpersonal communication include:

- barriers caused by perception;
- semantic barriers;
- non-verbal obstacles;
- bad feedback;
- inability to listen.

Obstacles in organizational communications are:

- distortion of messages;
- information overload;
- unsatisfactory structure of the organization.

The article will consider obstacles in organizational communications in the police sphere.

The first point may be the distortion of messages, this is when information moves inside the organization up and down, the content of messages is somewhat snake-like. This change may be due to completely different reasons. Messages can be distorted accidentally due to difficulties in contact between individuals. When the manager does not agree with the information, the message may deliberately distort the information. In this case, he modifies the message so that the change of content is in his interest.

Distortion of messages can cause problems with the exchange of information can also be due to filtering. In each organization, the information they receive is filtered so that the correct message is then sent to the correct department of the organization or to another level.

In order to speed up the movement of information in the organization, a variety of information is simplified before being sent to different segments of the organization.

Through the status of the organizational structure, it seems that when you go up the hill, you can become up-and-down.

Often, the status of the organization's rank, as a result of the development of a tendency to give positive information. "bazhana (not positive) information". The next rank is to see those who are, if they give me the opportunity to talk to their boss about that information for the sake of taking the stink out of the way, for those who want it.

It is important to take into account the most popular reason for the distribution of information.

Language adviser A. V. Bilousov

UDC [811.111:351.74(100)](06)

Iлона TYMOFIENKO

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN POLICE

An important role in the activities of law enforcement agencies is played by crime. The fight against crime is being waged in all countries, by various state organizations, enterprises, and citizens. Crimes should be prevented at an early stage, when the offender is only planning and planning to commit a certain act.

To date, the effectiveness of law enforcement depends on the technical equipment. To be more precise, in the practical activities of the National Police of Ukraine, computer technology, automated workplaces, which are equipped with modern personal computers and a large database, are widely used. This helps practical workers, they perform less monotonous work, ie all the work is entrusted to technical equipment. Today, technology helps to find solutions to various problems, gives the opportunity to study processes more widely, to analyze them.

In the conditions of growing computerization, including in the National Police of Ukraine, the main goal of the development process is to provide cadets, students and trainees of higher education institutions of the Ministry of Internal Affairs of Ukraine, employees of the National Police with special knowledge, skills and skills in innovative technologies and information support. their professional activity, which effectively use computer equipment and modern information technologies in their operational and service activities.

Instant chat is an important tool for real-time communication with sick or masked patients, as well as the deaf. And location services are based on the location of the subscriber's device, which allows you to determine exactly where the person is. Although it is necessary to have a special permit from the relevant institutions to track people, there are at least three ways to find out a person's location by phone number. This is sometimes necessary when you need to find a lost child or a wanted criminal. Searching for people by phone number is possible through specialized programs. This knowledge needs to be improved and developed through information technology.

When COVID struck, many officers realized that instant chat also helped them reduce the need for face-to-face meetings for routine police work that could be done over the phone.

Although these technologies were created or improved to help law enforcement adapt to the changing conditions of the COVID-19 pandemic, many of these problems existed before the pandemic and will continue to exist as the world adjusts to the new norm.

Simplified processes will lead to greater security for law enforcement officers and the people they serve, awareness of innovative technologies needs to be improved, then location accuracy will improve, instant chat features will develop faster, and workstations equipped with modern personal computers will become more automated and a large database, then public confidence in law enforcement will increase, and this is the main thing.

Language adviser A. V. Bilousov

UDC 351.74:001.895](100)(06)

Arina USENKO

Kharkiv National University of Internal Affairs

AUTOMATIC DEVICES IN THE SERVICE OF POLICE

Automation is a broad concept that describes all processes that are performed automatically using software or robots. That is, these are tasks that are performed without human intervention. Robotization covers the part of this practice, when physical mechanisms come to replace people.

The arrival of government-operated autonomous police robots does not look like predictions in science fiction movies. An army of robots with gun arms is not kicking down your door to arrest you.. Police robots may not be able to hurt people like armed predator drones used in combat and, as history shows, calling the police on someone can prove equally deadly.

Police Robots are designed to allow access to situations that are inaccessible or dangerous for first responders, and can manipulate objects as well as gather data through a variety of technologies. It covers robots suitable for a range of environments with varying data and communication capabilities.

For example, Knightscope's robots need cameras to navigate and traverse the territory. According to the proposal that the police department of Huntington Park, California, sent to the mayor and city council, these robots are equipped with many infrared cameras capable of reading license plates. They also have wireless technology capable of identifying smartphones within its range down to the MAC and IP addresses.

Police are receiving a lot of attention for testing robot “dogs,” which they have deployed in several situations, including food delivery in a hostage situation and searching the location where the police feared a dangerous gunman might be lurking.

Language adviser L. I. Rusanova

UDC 351.74:001.895](100)(06)

Illia USTYMENKO

Kharkiv National University of Internal Affairs

INNOVATIVE POLICE TECHNOLOGIES

The 21st century introduced new tools and categories to fight crime. Technology is transforming, and more and more police departments are deploying drones as eyes in the sky. In 2016 these technologies were just rolling out across agencies, and now, with the rapid pace of technological developments, agencies are finding new and innovative ways to leverage these tools to enhance public safety, catch criminals and save lives.

Drones, body-worn cameras, facial recognition software, artificial intelligence, and many others are the most important technologies that are equipping law enforcement agencies with new capabilities to protect and serve.

Facial Recognition Software is one of the more controversial emerging police technologies. When this tool first made its way into law enforcement, many people were concerned that it would be used unethically. Thankfully, that has not been the case, and facial recognition is proving to be an effective investigative tool.

The goal of facial recognition software is that it will help improve safety and security in a number of instances. NYPD officers were able to find and arrest a rape suspect within 24 hours of the attack using facial recognition software. And, because facial recognition is so promising, the U.S. Department of Homeland Security predicts that it will be used on 97 % of travelers by 2023.

Police have been using fingerprints to identify people for more than a century. Now, in addition to facial recognition and DNA, there is an ever-expanding array of biometric (and behavioral) characteristics being utilized by law enforcement and the intelligence community. These include voice recognition, palmprints, wrist veins, iris recognition, gait analysis and even heartbeats.

Language adviser L. S. Sazanova

UDC 351.74:001.895](100)(06)

Sofia VASYLCHENKO

Kharkiv National University of Internal Affairs

AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM USE IN POLICE WORK

Letters and numbers on license plates of vehicles help law enforcement officers determine if vehicles were stolen or if the owners are wanted. New technology streamlines this process. The automatic license plate recognition (ALPR) system is an integrated camera-database technology, meaning the system takes a picture of a car's license plate and then processes the numbers and letters against a known database, alerting the officer if a vehicle is suspicious.

The ALPRs can, with greater accuracy and no fatigue factor, identify, screen and record the license plates of more vehicles than an entire squad of police officers could handle. That means more wanted vehicles apprehended in less time, making this piece of law enforcement technology something no officer wants to do without.

The ALPRs use a combination of cameras and computer software to indiscriminately scan the license plates of every car passing by. The readers, which can be mounted on stationary poles, moving police cruisers, and even handheld devices, log the time and date of each scan, the vehicle's GPS coordinates, and pictures of the car. Some versions can also snap pictures of a vehicle's occupants and create unique vehicle IDs.

The devices send the data to ALPRs software, which can compare each plate against a designated "hot list." Such lists can include stolen cars and cars associated with AMBER Alerts for abducted children. They can also reference vehicles that are listed in local and federal databases for reasons that may include unpaid parking tickets or inclusion in a gang database. These queries happen automatically, though officers can also query plates manually. In addition to checking data in real time, many cities and agencies retain plate information for future use, sometimes indefinitely. This data can be used to plot a particular vehicle's various locations or to identify all the cars at a given location, and it can even be analyzed to predict routes and future locations of a vehicle or set of vehicles.

It would have been virtually impossible for law enforcement to surveil routinely all drivers. However, with the growing use of ALPRs, police can now receive alerts about a car's movements in real time and review past movements at the touch of a button.

Language adviser A. E. Korshenko

UDC [811.111:351.74(100)](06)

Vadim VLASOV

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN THE POLICE

An important role in the activities of law enforcement agencies is played by crime. The fight against crime is being waged in all countries, by various state organizations, enterprises and citizens. It is necessary to prevent crimes at the initial stage, when the offender only plans and plans to commit a certain act.

To date, the effectiveness of law enforcement depends on technical equipment. To be more precise, in the practical activities of the National Police of Ukraine, computer technology is widely implemented, automated workstations, which are equipped with modern personal computers and a large database. This helps practitioners, they do less monotonous work, ie all the work is entrusted to technical equipment. Today, technology helps to find solutions to various problems, gives the opportunity to more widely study the processes, to analyze them.

In the conditions of growing computerization, including in the National Police of Ukraine, the main goal of the development process is to provide cadets, students and trainees of higher education institutions of the Ministry of Internal Affairs of Ukraine, employees of the National Police with special knowledge, skills and information technology. their professional activities, which effectively use computer technology and modern information technology in their operational and service activities.

Instant chat is an important tool for real-time communication with sick or masked patients, as well as the deaf. And location services are based on the location of the subscriber's device, which allows you to determine exactly where the person is. Although it is necessary to have a special permit from the relevant institutions to track people, there are at least three ways to find out a person's location by phone number. This is necessary when you need to find a lost child or a wanted criminal. Searching for people by phone number is possible through specialized programs. This knowledge needs to be improved and developed through information technology.

When COVID struck, many officers realized that instant chat also helped them reduce the need for face-to-face meetings for routine police work that could be done over the phone.

Although these technologies were created or improved to help law enforcement adapt to changing conditions through the COVID-19 pandemic, many of these problems existed before the pandemic and will continue to exist as the world adapts to the new norm.

Simplified processes will lead to greater security for law enforcement officers and the people they serve, need to raise awareness of innovative technologies, then improve location accuracy, develop instant chat features faster, automate more workstations equipped with modern personal computers and a large database, then public confidence in law enforcement will increase, and this is the main thing.

Language adviser A. V. Bilousov

UDC 351.74:001.895](100)(06)

Serhii YUDIN

Kharkiv National University of Internal Affairs

GUNSHOT DETECTION SYSTEMS USE IN US CITIES

Now being implemented in a few US cities, the gunshot detection systems (GDS), or ShotSpotter, is a system that shows police officers where a gunshot has just been fired. This new and still-improving technology uses sensitive audio sensors placed around a neighborhood to detect gunshots and show officers the exact location. This law enforcement technology helps officers respond faster to gunshot incidents, which gives them a leg-up on assisting victims and tracking down suspects. GDS technology has the potential to make communities much safer, especially in areas where there are not enough officers to be on patrol.

The system shows almost instantly the location of where a gun fired to within 25 meters (82 feet). Already used by cops in several other US cities, ShotSpotter technology utilizes strategically placed audio sensors that relay gunshot location information to nearby cops, enabling a rapid response. The system, which costs \$1.5 million a year to set up and operate, is also smart enough to predict where subsequent shots may take place, allowing officers to approach a situation with the appropriate amount of caution and backup.

ShotSpotter is deployed overwhelmingly in communities of color, which already disproportionately bear the brunt of a heavy police presence. The police say they pick neighborhoods for deployment based on where the most shootings are, but there are several problems with that. First, ShotSpotter false alarms send police on numerous trips (in Chicago, more than 60 times a day) into communities for no reason and on high alert expecting to potentially confront a dangerous situation.

The placement of sensors in some neighborhoods but not others means that the police will detect more incidents (real or false) in places where the sensors are located. That can distort gunfire statistics and create a circular statistical justification for over-policing in communities of color. Second, ShotSpotter's methodology is used to provide evidence against defendants in

criminal cases, but is not transparent and has not been peer-reviewed or otherwise independently evaluated. That simply is not acceptable for data that is used in court. Finally, still up for debate is whether ShotSpotter's technology is even effective it's hoped ShotSpotter will help police to build an accurate picture of just how much gun activity there is in the cities.

Language adviser A. E. Korshenko

UDC [811.111:351.74(100)](06)

Nataliia ZADOROZHNA

Kharkiv National University of Internal Affairs

THE USE OF INNOVATIVE POLICE TECHNOLOGIES AS EXEMPLIFIED BY UKRAINIAN AND THE UNITED STATES POLICE

The fight against crime in Ukraine is being waged on a broad front by various state bodies and public organizations. An important role in this activity belongs to law enforcement agencies, for which the fight against crime is the main function.

Largely, the effectiveness of law enforcement depends on technical equipment. Today, computers are widely introduced into the practice of the National Police of Ukraine, local networks are created and automated workstations are equipped with modern powerful personal computers and databases. All this frees practitioners from monotonous operations, helps to find optimal solutions to various problems, allows for deeper study of processes, detailing them, and provides the opportunity to simultaneously consider a significant number of interrelated facts and dependencies in the simultaneous processing of various information.

However, innovative technologies in Ukraine have not yet reached a high level. The patrol police, when resorting to police measures, in particular to stopping vehicles, may encounter an inadequate and sometimes dangerous reaction from the driver. In the United States, where the carrying of a weapon is a constitutional right of an individual, such cases are not uncommon.

That is why a traffic stop robot was invented as an analogue that can act instead of a real person and reduce the risks of using firearms. Functional work includes scanning of driver's licenses, issuance of penalty receipts and detention of drivers by means of «spike arm».

Thus, information technology is an integral part of the police in various countries to fight crime and experience of various countries should be studied and implemented.

Language adviser N. V. Krasnova

UDC [811.111:351.74(100)](06)

Olena ZAHORUIKO

Kharkiv National University of Internal Affairs

A POLICE ROBOT AT THE CALIFORNIA LAW ENFORCEMENT SERVICE

Law enforcement has always been and remains fundamental to any civilized democratic society. All stages of development of society inevitably lead to the modernization of law enforcement, and the development of technology requires law enforcement agencies to take a new approach to the performance of daily duties, to regularly update the methodology for creating conditions for safe living.

American engineer Ruben Brewer from the non-profit research institute SRI International (California, USA) has created a robot that will help the traffic police. The prototype has passed the first tests, it is able to check the documents of the driver and issue penalty receipts.

Every year, U.S. police inspect several million drivers and vehicles. Physical force was used more than 190,000 times during the inspection. More than 4,000 employees were attacked, some killed. With this development, the robot becomes a necessary solution. The robot consists of a "body" with a document scanner, a printer and a "head" in an iron "cap" with a camera and a screen for communicating with the driver. After stopping the car under test, the robot "goes" to the driver's window and examines it with a video camera. The documents are checked using a scanner, and the built-in printer can print a receipt. If necessary, the patrol operator can talk to a suspicious driver through work. To prevent a potential intruder from escaping during the inspection, the robot sets a bar with spikes under the bottom of the car.

In conclusion, it can be noted, that innovative technologies are the key to the development of law enforcement, a tool that is becoming a real weapon in the fight against crime. Thanks to the proposals and recommendations developed by scientists and law enforcement specialists, as well as the joint efforts of foreign partners, deputies, government officials, heads of interested agencies can ensure real implementation of all innovations that will reduce crime.

A country that will have powerful information resources, an effective system for their implementation, will know the dynamics and prospects of their development, will be on the crest of scientific and technological progress and will be able to use it effectively.

Language adviser N. V. Krasnova

UDC [811.111:351.74(100)](06)

Oleksii ZHIZHIRIY

Kharkiv National University of Internal Affairs

HACKING: TYPES AND SECURITY

A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals. Hacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity. A traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. But this narrow view does not cover the true technical nature of hacking. Hackers are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cybersecurity software and IT teams. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data. As a result, modern-day hacking involves far more than just an angry kid in their bedroom. It is a multibillion-dollar industry with extremely sophisticated and successful techniques.

There are typically four key drivers that lead to bad actors hacking websites or systems: (1) financial gain through the theft of credit card details or by defrauding financial services, (2) corporate espionage, (3) to gain notoriety or respect for their hacking talents, and (4) state-sponsored hacking that aims to steal business information and national intelligence. On top of that, there are politically motivated hackers—or hacktivists—who aim to raise public attention by leaking sensitive information, such as Anonymous, LulzSec, and WikiLeaks. A few of the most common types of hackers that carry out these activities involve: Black Hat Hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign. White hat hackers can be seen as the "good guys" who attempt to prevent the success of black hat hackers through proactive hacking. They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking. Grey Hat Hackers

Grey hat hackers sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially.

There are several key steps and best practices that organizations and users can follow to ensure they limit their chances of getting hacked: software update, use unique passwords for different accounts, HTTPS Encryption, avoid clicking on ads or strange links, change the default username and password on your router and smart devices

Language adviser V. V. Kochyna

UDC [811.111:351.74(100)](06)

Valeriia ZHURBA

Kharkiv National University of Internal Affairs

INNOVATIVE TECHNOLOGIES IN THE SERVICE OF LAW ENFORCEMENT IN CHINA

Chinese police have begun using sunglasses equipped with special facial recognition technology to detect suspects.

The glasses are connected to an internal database, which means officers can quickly scan crowds while searching for fugitives.

Facial recognition technology is necessary for law enforcement agencies to find criminals, to provide security in crowded places, and to analyze big data, it is not an invasion of privacy because the pictures are taken in public places, the companies that developed them said.

"The camera is capable of covering 200 people at a time. The system has a database of wanted persons. The system is able to compare photos and signal when there is a match," said a company spokesman.

According to Chinese state media, the sunglasses have already helped police capture seven suspects.

The technology allows police officers to take a photo of a suspicious person and then compare it with photos stored in internal data. If there is a match, the person name and address information will be sent to the officer.

The glasses also support voice recognition and gesture control. With all these features, GLXSS weighs only 55 g. The glasses have a 0.25-inch VGA resolution viewfinder built into them.

All police officers at the station now use the smart glasses for quick identity checks. To date, police have managed to catch 7 fugitives and 26 fake ID holders at this station.

China is a world leader in facial recognition technology and regularly reminds its citizens that it is virtually impossible to get away with such equipment.

Language adviser G. S. Babak

UDC [811.111:351.74(100)](06)

Danylo ZHYRONKIN

Kharkiv National University of Internal Affairs

TECHNOLOGY AND POLICE IN THE NETHERLANDS

Since 2013, the Netherlands has one national police force with 10 regional units and one central unit. Since that time, more insight into technological developments within the police organization has been obtained, and innovation processes have been initiated more centrally. In 2016, an inventory revealed 130 technological projects that were carried out by the National Police of the Netherlands (Ernst and Kop, 2018). Only a small part of the projects reached the innovation stage, in which technology was implemented in operational police practice. Police organizations also need to prepare for future developments and adoption of technology in order to maintain legitimacy in this rapidly changing environment. The police must have insight into and an overview of the technology it uses and develops and of its effects in relation to societal developments, such as the use of bodycams. What factors promote or inhibit technological innovation processes from initial inception to implementation within the National Police of the Netherlands?

Today, technologies develop rapidly and reinforce each other. New technologies such as artificial intelligence, big data applications, the Internet of Things, mobile internet, robotics, autonomous vehicles, cloud technology, energy storage, and 3D printing have a major impact on national and international security, producing new or different forms and targets of crime. To cope with these new security issues and new forms of crime, the police will have to move along and adapt their organization and working methods accordingly. Technology also provides new promising tools for police officers.

New and innovative technology is often already developed and ready for use by the police organization, but getting the police to actually start using the technology proves to be difficult and depends on many social and organizational factors that are of decisive importance, as shown. The actual use of technology in the daily routine of police practice depends on flexible and customized support from facilitating services, the motivation and perseverance of project leaders and police chiefs, a clear organizational structure, and governance and the related timely and fitting decision-making on project development. Overall, the police organization needs a clear innovation strategy and vision on technology.

Language adviser I. O. Gogol

ТЕЗИ НІМЕЦЬКОЮ МОВОЮ

UDC 351.74:001.895](100)(06)

Oleksandra BORYSIUK

Charkiwer Nationale Universität des Innern

UAV FÜR ÖFFENTLICHE SICHERHEIT UND STRAFVERFOLGUNG

Der Einsatz moderner Technologien von Strafverfolgungsbehörden bietet neue Möglichkeiten, die Sicherheit der Bürger zu gewährleisten. Die Einführung der neusten Technologien in die Polizeiarbeit wird hauptsächlich von der Notwendigkeit getrieben, sich der Welt der Kriminalität zu stellen, die immer besser bewaffnet wird.

Im 21. Jahrhundert werden Drohnen von Polizeieinheiten in vielen Ländern der Welt eingesetzt. Drohnen gaben den Strafverfolgungsbehörden neue Möglichkeiten zur Beobachtung, zur Koordination von Einsatzmaßnahmen, zur Analyse der Situation, zur Suche nach Rechtsübertretern und Opfern. Im Dienst der Polizei stehen sowohl kompakte flugfertige Quadrocopter als auch komplexe multifunktionale unbemannte Systeme. Die Ausrüstung, womit diese Geräte ausgestattet werden können, stellen sicher, dass sich unabhängig von Tageszeit und Wetterlage folgende Aufgaben aus der Luft erfüllen lassen: das Patrouillieren und Beobachten großer Gebiete, das Suchen und Aufspüren von Personen mit einer Wärmebildkamera, die Überwachung der Ordnungsmäßigkeit bei öffentlichen Veranstaltungen, die Überwachung und die Analyse der Verkehrslage und der Unfallstellen, die Koordinierung von Polizeiaktionen.

Der Einsatz von UAVs hat eine Reihe von Vorteilen für die Polizeiarbeit. Die Motoren der Drohnen erzeugen nicht viel Lärm und stören die Bürger bei öffentlichen Veranstaltungen mit Geräuschen nicht. Polizeihubschrauber sind in mehrstöckigen Städten in Flughöhe und Manövrierfreiheit eingeschränkt. Die Drohne fliegt nicht nur frei zwischen Gebäuden, sondern ist auch in der Lage, direkt von Standorten innerhalb einer Siedlung abzuheben. Die Einsatzzeit des Quadropters beträgt wenige Minuten, er passt in den Kofferraum eines Autos und ist im Interesse der Polizei immer einsatzbereit. Drohnen erfordern ein Minimum an Spezialwissen. Ein Software-Update steht jedem PC-Benutzer zur Verfügung. Nutzlastelemente wie Kameras, Wärmebildkameras, Scheinwerfer und Lautsprecher können in wenigen Minuten installiert werden. Drohnen können in jeder Abteilung eingesetzt werden und lösen Probleme schnell, sicher und diskret mit minimalen Betriebskosten.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Oleksandr DAVYDOV

Charkiwer Nationale Universität des Innern

DIGITALISIERUNG DER POLIZEIARBEIT

Die Modernisierung der Forensik schreitet voran. Es entstehen neue Techniken, Mittel zum Aufspüren und Sicherung von Spuren am Tatort, spezielle Geräte und Ausrüstungen. Die Technologien werden von Jahr zu Jahr perfekter. Der Einsatz moderner Technologien durch die Strafverfolgungsbehörden bietet neue Möglichkeiten zur Gewährleistung der Sicherheit der Bürger. Die modernen Informations- und Kommunikationstechnologien haben unseren Alltag erobert, ihn effizienter, effektiver, flexibler und dynamischer gemacht.

Jeder, der moderne Technik nutzt, wirft einen digitalen Schatten. Er wird unter Berücksichtigung aller Informationen erstellt, die der Nutzer im Internet hinterlässt – die sogenannten Metadaten. Big-Data-Technologien werden von Strafverfolgungsbehörden verwendet, um soziale Prozesse in der Gesellschaft zu überwachen, Verbrechen vorherzusagen und zu verhindern. Dies umfasst die forensische Recherche von Informationen von mobilen Geräten: Daten zu ein- und ausgehenden Anrufen, Kontakten, empfangenen und gesendeten Nachrichten, einschließlich solcher, die in verschlüsselter oder versteckter Form enthalten sind usw.

Die Einführung digitaler Technologien in die Polizei wird weitgehend durch die Notwendigkeit getrieben, sich einer zunehmend bewaffneten kriminellen Welt zu stellen. Die Kriminellen nutzen aktiv die neuesten Errungenschaften der vierten industriellen Revolution. Die Folgen von Kriminalität, die in der Polizeiarbeit berücksichtigt werden müssen, werden immer breiter und schwerwiegender.

Die meisten Verbrechen werden mithilfe von Videoüberwachungssystemen aufgeklärt. Zurzeit beschäftigt man Video-Kameras, deren Daten im „Einheitlichen Datenspeicher- und Verarbeitungszentrum“ gesammelt werden. CCTV-Aufzeichnungen können als wertvolles Material für Strafverfahren verwendet werden. Die Polizei benutzt heute aktiv Drohnen. Ausgestattet mit einer Videokamera, werden sie dort eingesetzt, wo der Polizeibeamte in Gefahr sein kann. Die Drohnen sind in der Lage, auch an der Verfolgung von Kriminellen teilzunehmen.

Die Digitalisierung der Polizeiarbeit ist ein dynamischer Prozess. Die modernste Technologie ist in einer digitalisierten Welt für die Polizei unabdingbar. Der Einsatz dieser Technologien ermöglicht es der Polizei, ihre Aufgaben effizienter zu erfüllen und das Vertrauen der Bürger zu stärken.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Alona DOVBYSH

Charkiwer Nationale Universität des Innern

MÖGLICHKEITEN DER KÜNSTLICHEN INTELLIGENZ IM STRAFVERFOLGUNGSSYSTEM

Die Sicherheit ist ein menschliches Grundbedürfnis. Sie wird von Strafverfolgungsbehörden, Verkehrspolizei und Sicherheitsdiensten gewährleistet.

Die Verkehrssicherheit: In Großbritannien und Australien verwendet die Polizei beispielsweise neue Straßenkameras, mit deren Hilfe die Fahrer verfolgt werden, die während der Fahrt telefonieren. Diese Technologie beruht auf sensorbasierten Radarsystemen, die Fahrer durch die Windschutzscheibe fotografieren.

Das Beobachten von Großobjekten: Die Software in diesem Sektor richtet sich an Energie-, Versorgungs-, Kraftwerks-, Wasser- und Nuklearanlagen. Digitale Sicherheitslösungen kombinieren seismische, drahtlose und optische Sensoren mit Wärmebildkameras und der Videoanalyse und bieten einen vollständigen Überblick über den geschützten Bereich. Das System wird ausgelöst, wenn ein Einbruch erkannt wird. Betritt ein Fahrzeug oder eine Person einen verbotenen Geländeraum oder verweilt man dort länger als erlaubt ist, wird ein Alarm ausgelöst.

Die Sicherheit öffentlicher Veranstaltungen: die Verhinderung von Unruhen und Terroranschlägen, die Gewährleistung der Sicherheit bei Konzerten oder anderen großen Menschenansammlungen – auch für solche Aufgaben werden spezielle Systeme mit der Gesichtserkennungsfunktion entwickelt. Stellt sich heraus, dass ein Besucher für die Polizei oder andere Dienste von Interesse ist, werden sein Bild und seine persönlichen Daten auf dem Tablet des Sicherheitsbeauftragten angezeigt und rot markiert.

Die Überwachung von Privathäusern und Wohnungen: Künstliche Intelligenz getriebene Heimsicherheitssysteme sind die modernste Art, private Häuser und Wohnungen zu bewachen. Ein solches System ist in der Lage, Gesichter, Gegenstände und menschliche Figuren zu erkennen. Wird das Gesicht von der künstlichen Intelligenz innerhalb von 20 Sekunden nicht erkannt, wird die Sirene aktiviert und ein Notruf bei der Polizei abgesetzt.

Was ist das Endergebnis? - Intelligente Sicherheitssysteme, die von Polizeikommandozentralen verwaltet werden, sind bei der Überwachung, Kriminalitätsvorbeugung und der Verhinderung von Terroranschlägen wirksam. Der Einsatz solcher Systeme diszipliniert die Gesellschaft und erhöht die öffentliche Sicherheit.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Oleksandr DZHYHA

Charkiwer Nationale Universität des Innern

METHODEN DER 3D-TATORTDOKUMENTATION

Viele Wissenschaftler arbeiten daran, neue Methoden und Mittel zur Aufklärung von Verbrechen zu entwickeln. Von großer Bedeutung ist die Tatortarbeit der Ermittler gleich nach dem Verbrechen, aber nur ein kleiner Teil der Kriminalisten, die an der Aufklärung mitarbeiten, sind direkt am Ort des Geschehens und bei der Spurensicherung. Viele von ihnen machen sich erst später das Bild des Ereignisses. Dabei ist eine spezielle Ausrüstung sehr behilflich.

Die neueste Errungenschaft ist eine 360-Grad-Spheron-Kamera, mit der der Tatort abgeleuchtet wird. Das Gerät bietet eine Auflösung von 50 Millionen Pixel und einen 400-fachen Zoom. Es gibt die Möglichkeit, in abgedunkelten Räumen kleinste Details taghell darzustellen und Tatorte als ein vollständiges dreidimensionales Modell zu dokumentieren. So einfach und schnell eine Repräsentation mittels 360-Grad-Fotografie zu sammeln, ist eine Möglichkeit, die Genauigkeit der Tatortdokumentation durch den Einsatz der Technologie deutlich zu verbessern. Solche 3D-Modelle werden als Mittel zur dauerhaften und vollständigen „Konservierung“ der räumlichen Situation an Tatorten eingesetzt.

In einem Interview erläuterte Mehzeb Chowdhury, Doktor der Forensik und Kriminalrecherche an der Universität Durham, die Probleme mit Szenenverschlechterung des Tatortes und persönlichen Besuchen: „Der problematischste Aspekt von Tatortbesuchen ist, dass sich mit der Zeit jede Charakteristik der Szene in irgendeiner Weise ändert. Dies wird Szenenverschlechterung genannt. Eine zeitgleiche Momentaufnahme des gesamten Tatortes würde die notwendigen Details für Ermittlungen und Gerichtsverfahren bewahren. Personen, die nie am Tatort waren, können sich jederzeit ein wahrheitsgetreues Bild davon machen. Mit dieser Technologie steht die Information in realitätsnäherer Form zur Verfügung.“

Technologie spielt seit langem eine wichtige Rolle bei der Strafverfolgung. Und jetzt, mit der Reifung von 360-Fotografie und virtueller Realität, ist der Wiederaufbau der Tatorte genauer als je zuvor. Die am Tatort hergestellten 3D-Modelle sollen im Rahmen des Hauptverfahrens vor Gericht das Verständnis für räumliche Lagebeziehungen von Spuren unterstützen und die Datenbasis für eine intuitive Fallillustration liefern. Darüber hinaus fördern sie sowohl die Objektivität des Richters hinsichtlich des Beweismaterials als auch die Rechtssicherheit für den Verurteilten.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Yelyzaveta KOVALENKO

Charkiwer Nationale Universität des Innern

VIRTUAL REALITY IN DER VERKEHRSUNFALLPRÄVENTION

Die Verhütung von Verkehrsunfällen gehört zu den Aufgaben der Verkehrspolizei, die darauf abzielt, die Zahl der Verkehrsunfälle zu reduzieren und die Verantwortlichkeit der Verkehrsteilnehmer zu erhöhen. Die Unfallprävention im Straßenverkehr richtet sich an alle, insbesondere an gefährdete Verkehrsteilnehmer wie Radfahrer und Fußgänger.

Die Polizei Nordrhein-Westfalen startet ein Pilotprojekt zum Test von Virtual-Reality-Brillen. Dies eröffnet neue Möglichkeiten zur Verkehrsunfallvorbeugung. „Mit dem Einsatz der Virtual Reality Brillen heben wir die Präventionsarbeit bei Verkehrsunfällen mit schweren und schwersten Unfallfolgen im Straßenverkehr auf ein neues Level“, sagte Innenminister Herbert Reul. Die Polizei Nordrhein-Westfalen ist bei der Verkehrsunfallprävention bestrebt, Gefahren im Straßenverkehr „erlebbar“ zu machen. Durch den Einsatz einer Virtual-Reality-Brille wird es möglich, virtuell in eine Verkehrssituation einzutauchen.

In einem von der Polizei Nordrhein-Westfalen erstellten 3D-Film wird die Situation mit einem Radfahrer und einem Lkw-Fahrer gezeigt. Zuerst wird die Bewegungswahrnehmung eines Radfahrers als Nutzers der VR-Brille dargestellt, wenn er feststellt, dass der Lkw-Fahrer ihn im sogenannten „Toten Winkel“ aus den Augen „verliert“. In der zweiten Einstellung wechselt die Perspektive und man betrachtet die Abläufe aus der Sicht des Berufskraftfahrers. Die im Film gegebene Situation soll Verkehrsteilnehmern zeigen, wie aufmerksam sie während der Fahrt sein müssen und solche Momente berücksichtigen.

„Alternative Fortbewegung, wie das Radfahren oder auch die Nutzung von E-Bikes und Pedelecs, liegt voll im Trend und wird uns in der Verkehrsunfallprävention zukünftig noch stärker beschäftigen. Daher ist es gut und richtig bei unserem VR-Brillen-Projekt mit diesem Thema zu starten“, bekräftigt Minister Reul. „Radfahrerinnen und Radfahrer haben weder eine Knautschzone noch einen Airbag. Das können wir Ihnen mit unseren neuen technischen Möglichkeiten sehr plastisch vor Augen führen“.

Sicherheit ist ein menschliches Grundbedürfnis, für das die Polizei bereit ist, alles Notwendige zu tun. Die Prävention von Verkehrsunfällen hat ihre Vorteile, und moderne Technologien und Systeme der künstlichen Intelligenz sind hier von großer Bedeutung.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Viktoriia KULYK

Charkiwer Nationale Universität des Innern

EINSATZ VON HUBSCHRAUBERN IM POLIZEIDIENST

Die Bundespolizei betreibt eine Hubschrauberflotte, die hinsichtlich moderner Ausstattung, Effizienz und Größe in Europa ihresgleichen sucht. Helikopter werden eingesetzt, um solche Aufgaben wie Grenzpatrouillen und den Transport von Personal und Spezialkräften durchzuführen. Das Aufgabenspektrum der Polizeihubschrauberstaffeln umfasst die Suche nach Kriminellen, das Vermissten auffinden, den Schutz der öffentlichen Ordnung bei Massenveranstaltungen. Die Polizeihubschrauberstaffel leistet auch Unterstützungsarbeit für Spezialeinheiten der Polizei.

Der Haupthubschrauber der Flotte ist der EC155, ein 5 Tonnen schwerer Hubschrauber, der in einer Vielzahl von Operationen eingesetzt wird. Die Hubschrauberkabine bietet Platz für 13 Passagiere und zwei Piloten und kann bis zu 2 Tonnen schweres Gerät transportieren. Das moderne Cockpit ist mit digitaler Avionik und Autopilot ausgestattet.

Das niedrige Vibrationsniveau des Helikopters bietet ideale Voraussetzungen für den Einbau von Spezialausrüstungen der Polizei. Die Ausstattung der Bundespolizei umfasst Tag- und Nachtsichtkameras, leistungsstarke Flutlichter und Lautsprecher, ein 90 Meter langes Windenseil sowie ein System für Luftbild- und Videoaufnahmen. Daten und Aufzeichnungen werden direkt an die Kommando- und Lagezentralen der örtlichen Polizeidirektion und des Innenministeriums übermittelt.

Zur Hubschrauberflotte gehören neben dem EC155 B1 auch EC135 T2i Hubschrauber für Polizeiarbeit, Katastrophenhilfe und Rettungseinsätze, der AS332 L1 Super Puma Hubschrauber für Ferntransport, Luftraumüberwachung, VIP-Transport sowie EC120-Helikopter für Trainingsflüge.

Seit einigen Jahren haben Polizeihubschrauber ernsthafte Konkurrenten. Dies sind unbemannte Luftfahrzeuge. Sie sind einfacher und kostengünstiger, ideal für die visuelle Beobachtung des Geländes und von Straßenkreuzungen, aber die Fähigkeiten von Drohnen sind eigentlich nur auf diese Funktion beschränkt. Die Polizei setzt traditionelle Lufttransportmittel ein – Helikopter, Drehflügelflugzeuge werden weiterhin die Sicherheit der Bewohner von Großstädten und abgelegenen Regionen des Landes gewährleisten und eine hohe Einsatzbereitschaft garantieren.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Bohdana NESHTA

Charkiwer Nationale Universität des Innern

DIGITALE TRANSFORMATION IM BEREICH DER POLIZEITÄTIGKEIT

Die rasante Entwicklung der modernen Technik und der Kommunikationsmöglichkeiten eröffnet neue Möglichkeiten zur Begehung von Straftaten. Das Betätigungsfeld der Kriminellen ist umfangreich, es erstreckt sich vom Online-Betrug, Phishing, Identitätsdiebstahl, über Ausspähung von Daten bis zur gemeingefährlichen Computersabotage. Riesige digitale Datenbank wurde zu einer Herausforderung für die Sicherheitsbehörden. Vor den Polizeibeamten steht eine schwierige Aufgabe, die in der Suche nach Spuren und Beweisen für strafrechtlich relevante Handlungen in Netzen der Informations- und Kommunikationstechnik besteht. Eine immer größere Rolle spielen digitale Spuren in Computern, Kommunikationsgeräten und -netzen im Ermittlungsverfahren.

Der Einsatz moderner Informations- und Kommunikationstechnologien ist im polizeilichen Alltag alltäglich geworden. Die Arbeit im BKA und in der deutschen Polizei ist heute ohne funktionierende IT-Infrastruktur kaum vorstellbar. Von der Entwicklung spezieller Software für den Bedarf der Polizei über Big Data bis hin zu international vernetzten IT-Systemen wird das gesamte Spektrum der Informationstechnologien eingesetzt. Hochautomatisierte, vernetzte und smarte Systeme auf Grundlage von Digitalisierung, Robotik, Sensorik sowie Cyber-physischen Systemen und Big Data verändern alle Bereiche der Arbeitswelt der Polizei maßgeblich. Die digitale Transformation kommt zunehmend in der polizeilichen Tatortarbeitstechnologie zum Einsatz.

Der Bereich IT-Forensik als zentrale Service-Einheit des BKA unterstützt die Ermittlungen bei der Beweissicherung von Datenträgern und bereitet diese für die kriminalistische Auswertung auf. Ziel der Aktivitäten des Servicezentrums ist es, sowohl vorbeugende Tätigkeit zu fördern, etwa durch Beratung zu möglichen technischen Präventionsmaßnahmen, als auch Ermittlungen der Polizei auf technisch hohem Niveau zu unterstützen. Durch systematische und kontinuierliche Beobachtung entwickelte Technologien werden auf ihre polizeiliche Relevanz analysiert und in besonderen Fällen auch getestet. „Wollen wir Kriminalität wirksam bekämpfen, müssen wir bestrebt sein, uns die Zukunft zu vergegenwärtigen, um eine fundierte Risikoeinschätzung vorzunehmen. Dies setzt eine umfassende Früherkennung und Frühaufklärung voraus. (Jörg Ziercke).

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Yana SKRYPNYK

Charkiwer Nationale Universität des Innern

IRISERKENNUNG ZUR IDENTIFIZIERUNG VON PERSONEN

Die Beachtung wissenschaftlicher Erkenntnisse und die Verwendung von verschiedenen innovativen Programmen in der Tätigkeit der Rechtspflegeorgane sind sehr wichtig. Die Möglichkeit der Anwendung verschiedener neuer Technologien ist eine Grundlage der erfolgreichen Arbeit der Polizei. Die Iriserkennung ist eine Methode der Biometrie zum Zweck der Authentifizierung oder Identifizierung von Personen. Dafür werden mit speziellen Kameras Bilder der Iris des Auges aufgenommen, die charakteristischen Merkmale der jeweiligen Iris identifiziert und gespeichert bzw. mit einem oder mehreren bereits gespeicherten Templates verglichen. Im Vergleich zu anderen biometrischen Systemen wie Gesichtserkennung, Fingerabdruck, Sprache, DNA-Analyse wird die Iriserkennung als eine der zuverlässigsten Methoden betrachtet.

Zur Verfügung der Polizei stehen heute verschiedene Systeme zur Iriserkennung eines Menschen. Die Software zur Iriserkennung von DERMALOG bietet die notwendige Qualität und Genauigkeit zur Erfassung und Verwaltung einer Vielzahl an Iris-Bildern. Die gesammelten Daten werden zur Registrierung oder Verifizierung einer Person verwendet.

Als Beispiel kann ein System zur Iriserkennung eines sich bewegenden Menschen, welches die Identität eines Menschen anhand seiner Iris aus ca. 5 Meter Entfernung feststellen kann. Das Gerät ermöglicht es, eine Person ohne zusätzliche Verfahren oder Bemühungen der Person selbst zu erkennen, d.h. die Person muss sich nicht nähern und in den Scanner blicken.

All diese Eigenschaften haben die Iriserkennung zu einer attraktiven Technologie im Einsatz für Sicherheitsanwendungen gemacht. Viele Iriserkennungssysteme werden zur Erhöhung der Sicherheit mit anderen biometrischen Identifikationssystemen oder anderen Methoden zur Identifikationsüberprüfung kombiniert. Die Wahrscheinlichkeit, dass ein kombiniertes System zur Identifizierung von Fingerabdrücken und Iris umgangen wird, ist sehr gering. Andere Systeme stützen sich vollständig auf Iriserkennungssysteme, da sie ein sehr geringes Potenzial für eine fehlerhafte Identifizierung aufweisen. Diese Innovation kann in besondere Sicherheitszonen wie z.B. an Grenzübergängen dienlich sein. Sie eignet sich ebenfalls für den Einsatz in anderen Bereichen, wenn die Identität einer Person in einer größeren Menschenmenge bestimmt werden soll.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Yana TELUKHA

Charkiwer Nationale Universität des Innern

INNOVATIVE TECHNOLOGIEN IN DER POLIZEI

Die Entwicklung von Technologien kann man schwer vorhersagen. Frühzeitiges Wissen über potenziell aktuelle Technologien ermöglicht eine aktive Anwendung der damit verbundenen Chancen für innovative Einsatz- und Ermittlungstechniken. Die Erarbeitung neuer Methoden zum Aufspüren von Sprengstoffen, Rauschgiften, Waffen und sonstigen Substanzen mit Strafrelevanz sowie die systematische Erprobung von erhältlicher Detektionstechnik gehören zu den Kernaufgaben in diesem Arbeitsbereich. Neue technische Entwicklungen werden aktiv in die polizeiliche Aufgabenerledigung integriert.

Die individuellen biologischen Merkmale (Fingerabdruck, Stimme, Gesicht, Augen etc.) werden auch in der nahen Zukunft zur Identifizierung einer Person verwendet. Fingerabdrücke aber werden schon heute nicht mehr manuell verglichen, sondern durch Automatische Fingerabdruck-Identifizierungssysteme.

Moderne Technologien, Taktiken und neue Formen des Sammelns, der Speicherung und Weitergabe von Informationen sind heute längst zum polizeilichen Alltag geworden. Die Vergrößerung des Aufkommens an digitalen Daten stellt eine Herausforderung für die Sicherheitsbehörden dar. Diesem Prozess muss mit modernen intelligenten Analysemethoden entgegengetreten werden. Für polizeiliche Bedürfnisse kann dabei nicht immer herkömmliche Software verwendet werden. Oftmals werden daher spezielle Softwarelösungen und Methoden entwickelt.

Neue Informations- und Kommunikationstechnologien haben Umfang und Intensität der Polizeikontrolle verändert. Dazu gehören neue Versionen der Videoüberwachung: Sie ermöglichen es nicht nur, die Bewegungen einer Person quer durch ganze Gebäudekomplexe oder gar Innenstädte am Bildschirm zu verfolgen. Sie nutzen die Synergien anderer neuer Technologien – z.B. biometrisches Verfahren – und automatisieren die Kontrolle von Fahrzeugen oder Personen.

Die zunehmende Durchdringung aller Lebensbereiche mit moderner Technik und Kommunikationsmöglichkeiten eröffnet bislang ungeahnte Möglichkeiten zur Begehung von Straftaten. Das Bundeskriminalamt beobachtet den Fortschritt in diesem Bereich sehr intensiv und entwickelt selbst eigene Strategien und Methoden sowohl zur Vorbeugung als auch zur Strafverfolgung.

Sprachberaterin H. N. Sorokina

UDC 351.74:001.895](100)(06)

Uliana YANKOVSKA

Charkiwer Nationale Universität des Innern

VIRTUAL REALITY BEI DER POLIZEIAUSBILDUNG

Aus irgendeinem Grund wird angenommen, dass die Welt der Zukunft frei von der Kriminalität sein wird. Aber wird die Zeit wirklich kommen, in der es möglich sein wird, jedes Verbrechen aufzuklären, und es wird kein Verbrechen geben, das nicht hätte verhindert werden können?

Vor einigen Jahren kam die Idee, Strafverfolgungsbeamte durch Virtual Reality (VR) auszubilden, nicht in Frage. Heute ist die virtuelle Realität technisch ausgereift und die Technologie hat sich in vielen Berufen weit verbreitet. Diese Lerntechnologien können für eine sichere berufliche Entwicklung eingesetzt werden, um reale Risiken in der Zukunft zu vermeiden. US-Polizeibehörden führen spezielle Schulungen mit virtueller Realität durch. Solche Übungen helfen den Beamten, sich auf unvorhersehbare Einsatzszenarien vorzubereiten.

Polizeibeamte können sich in einem virtuellen Handelszentrum oder in einer öffentlichen Schule in der Situation, die mit der Geiselnahme verbunden ist, befinden. Gleichzeitig werden verschiedene Kampfszenarien, basierend auf realistischen Ereignissen, ausgearbeitet. VR ermöglicht es den Polizisten, verschiedene Szenarien in Echtzeit zu üben und mit virtuellen Objekten, einschließlich Partnern, zu interagieren. Dazu muss man eine Weste mit Sensoren und einen Virtual-Reality-Helm anlegen. Alle Polizeiaktionen werden zur weiteren Analyse aufgezeichnet.

Die Konstruktion kombiniert gleichzeitig eine Video- und Fotokamera sowie ein Navigationsgerät. Das Hauptmerkmal der virtuellen Reaktionsbrille ist die Erstellung eines virtuellen Bildschirms. Das Gerät ähnelt einer Sonnenbrille mit einer leichten Verdickung der Bügel, in denen Computerchips verbaut sind. Mit ihrer Hilfe können Polizisten zusätzlich die notwendigen Informationen erhalten. Wenn man beispielsweise die Straße darin überprüft, zeigt das Gerät die Anzahl der Autos auf dem Parkplatz an. Wenn ein Polizist seine Brille auf die Autonummer richtet, zeigt der Bildschirm möglicherweise Daten an, dass das Auto gestohlen wird.

Der Einsatz von Virtual Reality eröffnet neue Möglichkeiten für Polizisten. Der Umgang mit modernen VR-Geräten erfordert keine tiefgreifenden Kenntnisse in der Computertechnologie, wodurch sie leicht zu erlernen sind. Daher führen immer mehr Länder aktiv Augmented- und Virtual-Reality-Technologien in Polizeiausbildungsprogramme ein.

Sprachberaterin H. N. Sorokina

ТЕЗИ ФРАНЦУЗЬКОЮ МОВОЮ

UDC [351.74: 001.895(100)](06)

D. O. MEDIANYK

L'Université Nationale des Affaires Intérieures de Kharkiv

LA ROBOTIQUE AU SERVICE DE LA POLICE

Au cours des dernières années, l'humanité a fait de grands progrès dans le domaine de la technologie, qui a en fait touché toutes les sphères de l'activité humaine. Les pays les plus développés du monde commencent de plus en plus à utiliser des systèmes automatisés dans différents domaines, y compris les forces de l'ordre. Il est difficile d'identifier quel pays a vu la première utilisation de la robotique dans les postes de patrouille de police, mais pour le moment, les robots sont utilisés aux États-Unis, aux Émirats Arabes Unis, en Chine, au Kazakhstan, à Singapour etc.

Ainsi, en Californie, il est déjà possible de trouver des robots qui peuvent se déplacer pour analyser la situation comme calme ou dangereuse. Ces robots opèrent en tant qu'assistants ou policiers dans plusieurs centres commerciaux et bureaux de grandes entreprises technologiques.

Un autre appareil, appelé «le REEM work» et lancé aux Émirats Arabes Unis, peut protéger les gens contre les atrocités, car il peut diffuser immédiatement au centre de contrôle ce qui se passe. Les gens peuvent l'utiliser pour signaler un crime, payer des amendes et obtenir des informations en appuyant sur l'écran tactile.

Les technologies innovantes sont très importantes de nos jours, ce qui nous aide beaucoup à vivre (les smartphones qui peuvent nous parler, répondeurs, appareils intelligents et toutes les autres merveilles apportées grâce au développement de la technologie (D'après «Les nouvelles de France» <https://www.france24.com/fr>). Ainsi on a décidé en Tunisie que le robot policier patrouillerait dans les rues afin que les habitants de la ville ne violent pas les règles d'isolement. (D'après «le Portail du ministère de l'intérieur» <https://www.interieur.gov.tn>).

Robocop, qui se déplace sur roues est contrôlé à distance et équipé de caméras infrarouges et thermiques, ainsi que d'un système d'alarme sonore et lumineuse. Les bandes sonores et les vidéos, publiées sur le site du Ministère tunisien de l'Intérieur, nous montrent que le robot s'adresse à des individus soupçonnés d'avoir enfreint les règles de confinement: «Qu'est-ce que tu fais? Montre-moi ton passeport. Tu ne sais pas que tu dois rester chez toi?».

Le robot transmet un signal et une image de l'intrus, l'identifiant, au poste de police le plus proche.

Le créateur tunisien du robot, Anis Sahbani, a déclaré que le robot avait été lancé pour la première fois en 2015 pour patrouiller dans les rues. Selon lui, la machine automatisée fonctionne de manière autonome grâce à l'intelligence artificielle.

Le robot dans diverses modifications coûte de 100 à 140 mille dollars et il est vendu principalement à des entreprises étrangères pour des besoins de sécurité.

Au Japon, tels robots peuvent être utilisés presque partout, de l'épicerie aux laboratoires cliniques. Mais la question reste encore ouverte en ce qui concerne les robots programmés pour assurer l'ordre public.

Aujourd'hui il ne s'agit pas encore de l'utilisation généralisée des robots et de l'intelligence artificielle dans la police, le ministère de l'Intérieur de l'Ukraine n'est pas encore prêt à remplacer les policiers dans les rues par des robots. Mais une telle manifestation de la mise en œuvre des résultats de la révolution scientifique et technique est assez réussie et très prometteuse. Ce n'est qu'une question de temps. L'étude de l'expérience mondiale nous permet de conclure que l'utilisation des robots dans l'activité policière permet de rendre cette activité sûre et efficace. A mon avis, dans les activités d'application de la loi l'utilisation de la robotique dans les postes de patrouille de police serait un domaine prometteur.

Consulteur de langue **L. D. Diagilieva**

UDC [351.74: 001.895(100)](06)

J. R. SARVAEVA

L'Université Nationale des Affaires Intérieures de Kharkiv

MISE EN ŒUVRE DES MESURES OPÉRATIONNELLES DE RECHERCHE DANS LE CYBERESPACE

Aujourd'hui la société est dépendante des réseaux sociaux et passe la plupart de son temps sur Internet. L'environnement d'information interactif est formé à la suite du fonctionnement de systèmes de communication compatibles (connectés) et de l'utilisation de l'internet et/ou d'autres réseaux mondiaux de données. Les savants nomment cet environnement le cyberspace.

On doit réaliser que les internautes ne sont pas seulement des citoyens respectueux des lois. En utilisant des systèmes de communication et d'autres réseaux mondiaux de données les malfaiteurs peuvent porter atteinte au droit d'auteur, encourager la violence, commettre une fraude en ligne, distribuer de la pornographie vendre des drogues et des substances psychotropes etc. Les groupes criminels organisés restent en contact via Internet. Dans les conditions modernes, le cyberspace devient de plus en plus l'environnement, qui se caractérise des effets secondaires de nature criminogène.

Dans de nombreux pays, le cyberspace qui contient généralement des traces d'activités illégales de criminels, fait sans aucun doute l'objet de l'attention particulière des forces de l'ordre de ces pays.

Compte tenu de l'expérience étrangère et pour renforcer la lutte contre la criminalité les organes des affaires intérieures de l'Ukraine doivent élaborer et mettre en œuvre des mesures opérationnelles et de recherche appropriées dans le cyberspace.

A cet égard, il convient de distinguer la lutte contre la cybercriminalité elle-même et l'organisation des mesures opérationnelles et de recherche avec l'aide de cyberspace.

Les mesures ci-dessus peuvent être utilisées à la fois pendant les enquêtes menées dans l'espace virtuel et réel. Afin d'obtenir des informations inconnues et cachées d'intérêt opérationnel, les organes des affaires intérieures de l'Ukraine commencent à accorder de plus en plus d'attention au cyberspace.

Les activités des organes des affaires intérieures de la collecte et de l'analyse des informations placées dans le cyberspace sont visées à la recherche des preuves (sujets, circonstances) témoignant de la commission des crimes et leurs auteurs.

Suite de l'étude de la meilleure expérience étrangère il est possible de définir les directions de base de la mise en œuvre des mesures opérationnelles de recherche dans le cyberspace. Ainsi on diffère:

- 1) l'identification des personnes d'intérêt opérationnel;
- 2) la recherche des personnes spécifiques en établissant leur emplacement physique;
- 3) l'établissement des connexions secrètes;
- 4) la recherche d'objets volés et l'identification des personnes impliquées;
- 5) l'exercice d'une influence psychologique sur les participants des structures criminelles en menant un travail actif sur les forums et les chats.

Théoriquement, il est nécessaire d'établir une liste claire des mesures opérationnelles de recherche, de déterminer des services et des personnes concernés. Il convient de choisir les méthodes appropriées d'organisation des mesures opérationnelles de recherche dans le cyberspace. Nous considérons comme prometteuses les méthodes suivantes: l'analyse des sources d'information ouvertes, l'ingénierie sociale, la réception et l'analyse des informations des opérateurs et fournisseurs de télécommunications

A notre avis, la mise en œuvre des mesures opérationnelles de recherche dans le cyberspace sera plus efficace à condition que les organes des affaires intérieures de l'Ukraine utilisent d'une manière complexe leurs forces, moyens, mesures et méthodes. En plus, cette utilisation doit respecter toutes les conditions du respect stricte et rigoureux de la législation en vigueur et d'exclure toute la manifestation de violation des droits humains et civils.

Consulteur de langue **L. D. Diagilieva**

ТЕЗИ УКРАЇНСЬКОЮ МОВОЮ

УДК 351.74:001.895](100)(06)

Альона БЕРЕЖЕЦЬКА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Поліцейські технології перемістилися з адміністративної будівлі в ядро поліцейських операцій.

Сьогодні поліцейські управління використовують камери спостереження, системи виявлення пострілів, автоматизовані зчитувачі номерних знаків, програмне забезпечення для розпізнавання облич, камери тіла, дрони та численні бази даних для запобігання, реагування та розслідування злочинів.

Найближче майбутнє має ще більше можливостей, як-от безпілотні патрульні автомобілі з проекційними екранами, які передають інформацію, коли автомобіль патрулює вулиці. Доповнена реальність і штучний інтелект з часом знайдуть свій шлях у поліцію. Розумна поліцейська уніформа могла б контролювати рівень стресу офіцерів та навколишні умови та повідомляти про них, а також забезпечувати ситуаційну обізнаність керівників про своїх офіцерів.

Питання не в тому, чи існує ця технологія, а в тому, чи повинна поліція використовувати її, коли вона стане для неї доступною? І якщо так, то як його використовувати?

Ми вважаємо, що ці проблеми найкраще можна вирішити, розробивши та використавши систему цифрової етики та набір керівних принципів, які допомагають створити цифрову довіру. Така структура може допомогти керівникам поліції та їхнім зацікавленим сторонам продумати потенційний вплив технологій на офіцерів і громаду, виявити непередбачувані наслідки та вирішити питання щодо використання передових технологій для громадської безпеки.

Сьогодні успішний бізнес повинен розуміти соціальні та етичні наслідки використання технологій та роботи для пом'якшення негативних наслідків. Хоча це, можливо, необхідно для бізнесу, це неминуче справедливо для державного сектору, зокрема поліції. Подібно до того, як керівники поліції сьогодні працюють над створенням довіри у громаді, найближчим часом їм доведеться зайнятися створенням цифрової довіри.

Цифрова довіра створюється, коли організація має хорошу цілісність даних, безпеку та контроль, а використання нею технологій та

даних регулюється етичним кодексом. Цифрова довіра між поліцією та її зацікавленими сторонами може сприяти швидшому застосуванню перспективних технологій та пом'якшити деякі ризики, пов'язані з нею.

Цифрова етика є ширшою та включає як використовуються технології та дані та результати цього використання. Прозорі дані та цифрова етика створюють цифрову довіру.

Наступний фреймворк був розроблений Accenture. Наведено приклади елементів, що включають етику даних та цифрову етику. Це гарне місце для керівників поліції, щоб почати думати про цифрову довіру.

У міру того, як ми рухаємося далі в 21 столітті, цифрова етика та довіра стануть першочерговою проблемою для поліції. Ваші громади та ваші офіцери вимагатимуть, щоб збір даних, проведений аналіз та використання даних, аналізу та технологій були безпечними та етичними.

Останні приклади того, як цифрова етика і довіра можуть проявитися, можна знайти в Чикаго і Новому Орлеані. Управління поліції в обох містах пояснили, що вони використовують алгоритми для створення списків осіб із високим ризиком. Дві основні проблеми, які виникли в цих містах, були навколо прозорості в тому, які дані використовувалися і як був створений алгоритм, і як використовувалися результати.

Науковий керівник Н. Л. Горбач

УДК 351.74:001.895](100)(06)

Микита БЕЛЄВЦОВ

Харківський національний університет внутрішніх справ

ЕТИЧНЕ ПИТАННЯ ВИКОРИСТАННЯ ПОЛІЦІЄЮ КВАДКОПТЕРІВ У ЗОНІ ПРИВАТНОЇ ВЛАСНОСТІ

На даний момент, з розвитком безпілотних операцій, у зйомках матеріалів під час польотів на приватній території виникає етична проблема. У зв'язку з більшим використанням дронів як цивільними, так і державними установами, поліцейському департаменту важливо розробити ефективну політику щодо дронів. Тому необхідність правового регулювання пов'язана не з використанням дронів, а з потенційним порушенням недоторканності особистої власності.

Дрони, також відомі як безпілотні літальні апарати (БПЛА) або безпілотні авіаційні системи (БПАС), — це літаки, які літають без пілота на борту.

Правила використання дронів в Україні (для цивільних):

Безпілотники вагою до 20 кг можуть експлуатуватися без отримання заяв та дозволів на використання повітряного простору з дотриманням таких правил:

- максимальна висота польоту не вище 120 м над рівнем земної (водної) поверхні поза межами встановлених заборон та обмежень використання повітряного простору;
- польоти не виконуються над місцями скупчення людей на відкритому просторі та над густо забудованими районами;
- швидкість польоту дрона не більше 160 км/год;
- польоти виконуються не ближче 5 км від зовнішніх меж злітно-посадкових смуг аеродромів або не ближче 3 км від зовнішніх меж злітно-посадкової смуги/вертодромів;
- польоти виконуються не ближче 500 м від пілотованих літаків;
- польоти виконуються в межах прямої видимості (VLOS - візуальна лінія видимості);
- дрон не перетинає кордон України. У всіх інших випадках необхідний дозвіл на політ з чітко зазначеним маршрутом і цілями польоту, які видаються Державіаадміністрацією України.

Уповноважена забезпечувати дотримання законів, якими суспільство погодилося керувати, поліція має унікальне етичне ставлення до закону. Щоб дії поліції були етичними, вони спочатку мають бути законними. Закон є необхідним деонтологічним орієнтиром для офіцерів та органів у визначенні правильної та неправильної поведінки. На жаль, у сучасних умовах законодавчих актів, що регулюють використання БПЛА органами поліції, недостатньо. Ця обставина створює референційну порожнечу для керівників правоохоронних органів, які прагнуть застосувати технологію дронів на послуги населення. Відсутність чітко визначених етичних рамок використання дронів є як політичною дилемою, так і пробілом у знаннях. Політична дилема впливає з того факту, що технологія виходить за рамки регулювання. Ці закони часто сильно відрізняються, що призводить до невідповідностей від однієї юрисдикції до іншої в таких аспектах, як коли дрони можуть літати в повітряному просторі країни.

Оскільки перелік агенцій, які прагнуть використовувати дрони, буде розширюватися, потреба в політичному керівництві та структурі прийняття рішень зростатиме.

Консультант з мови Н. В. Краснова

УДК 351.74:001.895](100)(06)

Анастасія БУКІР

Харківський національний університет внутрішніх справ

ЩОБ БУТИ АДВОКАТОМ, ПОТРІБНІ ТРИ РІВНІ НАВИЧОК

Колись юридичні фірми вважали себе постачальниками послуг, але близько 20 років тому вони почали представляти себе як експертів з доступом до інформації, яка була недоступна їхнім клієнтам. З настанням цифрової ери все суттєво змінилося, і сьогодні клієнти очікують трохи більше. Нинішнє перетворення, зумовлене технологіями, інноваціями та співпрацею, призводить до створення цінних послуг. Тим не менш, юридичні фірми стикаються з проблемою: вони повинні прийняти нове мислення та придбати новий набір навичок, більш схожих на навички інноваторів, які підходять до вирішення проблем під іншим кутом зору. Юристи, як і будь-які інші професіонали, мають ряд характерних рис. Як і лідери, юристи зосереджені на вирішенні проблем і мають стратегічне бачення. Різниця полягає в тому, що юристи бойові, критичні, орієнтовані на правила, а їхня позиція за замовчуванням є змагальною. Навпаки, лідери творчі, чуйні, готові до співпраці та готові йти на ризик. Фахівці з права мають інтегрувати мислення лідерів та новаторів у свій спосіб роботи та надання послуг. Юристи повинні бути спостережливими, розвивати стосунки та будувати мережі, постійно ставлячи під сумнів усе у пошуках рішень.

Постачальники юридичних послуг повинні володіти трьома рівнями навичок. Щоб стати юристом, потрібні три рівні навичок:

Перший рівень складається з конкретних можливостей, пов'язаних з трьома факторами: організація, де працюють юристи або якій вони надають свої послуги; самі послуги; і технологічні фактори. Цей рівень включає навички, пов'язані з управлінням проектами, лідерством, технологіями, галузевими знаннями, бізнес-знаннями, маркетингом, комунікацією, публічними виступами та наставництвом, серед іншого.

Другий рівень включає в себе так звані навички «співробітництва», а також навички, пов'язані з творчістю, що важливо для пошуку кращих рішень. Навички цього рівня включають емпатію, інклюзивність, побудову стосунків, мислення щодо зростання, мультидисциплінарність, різноманітність та зухвалість — це лише деякі з них.

Третій рівень, що складається з навичок, орієнтованих на клієнта та обслуговування, є місцем, де відбуваються справжні інновації. Саме ці навички, які є справжнім джерелом лідерства, відрізняють фахівців з права серед інших.

Набуваючи навичок, необхідних, щоб бути юристом, більшість юристів традиційно зосереджувалися на розвитку навичок першого рівня. До другого шару було додано небагато зусиль, а третім шаром знехтували.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Інна БЛАГАДИР

Харківський національний університет внутрішніх справ

КРИПТОВІРУСНА ТЕХНІКА: ШКІДЛИВА ПРОГРАМА З ВИМОГОЮ ВИКУПУ

Програми-вимагачі – це тип зловмисного програмного забезпечення з криптовірусології, яке загрожує опублікувати персональні дані жертви або назавжди блокувати доступ до них, якщо не буде сплачений викуп. Хоча деякі прості програми-вимагачі можуть блокувати систему, не пошкоджуючи жодних файлів, більш просунуті шкідливі програми використовують техніку, яка називається криптовірусним вимаганням. Він шифрує файли жертви, роблячи їх недоступними, і вимагає сплати викупу, щоб розшифрувати їх. Під час правильно реалізованої криптовірусної атаки вимагання відновлення файлів без ключа дешифрування є важкорозв'язною проблемою – і важко відстежити цифрові валюти, такі як рауsafescard або біткойн та інші криптовалюти, які використовуються для викупу, що ускладнює відстеження та переслідування винних.

Атаки програм-вимагачів зазвичай здійснюються за допомогою трояня, замаскованого під легітимний файл, який користувач обманом завантажує або відкриває, коли він надходить як вкладення електронної пошти. Однак один гучний приклад, хробак WannaCry, автоматично переміщався між комп'ютерами без взаємодії з користувачем.

Шкідливе програмне забезпечення-вимагач спочатку було обмежено однією або двома країнами Східної Європи, а потім поширилося через Атлантику до Сполучених Штатів і Канади. Кількість кібератак у 2020 році була вдвічі більше, ніж у 2019 році. Перші версії цього типу шкідливого програмного забезпечення використовували різні методи для відключення комп'ютерів шляхом блокування системної машини жертви (Locker Ransomware). Програми-вимагачі використовують різні тактики для вимагання жертв. Одним із найпоширеніших методів є блокування екрана пристрою шляхом відображення повідомлення від відділення місцевих правоохоронних

органів про те, що жертва повинна сплатити штраф за незаконну діяльність. Програма-вимагач може запросити платіж, надіславши SMS-повідомлення на номер з преміальним тарифом. Деякі подібні варіанти зловмисного програмного забезпечення відображають вміст порнографічного зображення та вимагають оплати за його видалення. До 2011 року тактика програм-вимагачів змінилася. Зловмисники почали використовувати електронні способи оплати, а також мовну локалізацію на ураженому пристрої. Корпорації, приватні організації, уряди та лікарні можуть постраждати від цих зловмисних атак. У 2016 році було відзначено значний ріст атак програм-вимагачів на лікарні. Відповідно до звіту про загрози безпеки Інтернету за 2017 рік від Symantec Corp, програмне забезпечення-вимагач вплинуло не тільки на IT-системи, але й на догляд за пацієнтами, клінічні операції та виставлення рахунків. Злочинців в Інтернеті можуть мотивувати наявні гроші та відчуття невідкладності в системі охорони здоров'я.

Факторами, які є ключовими для успішної програми тренінгу з кіберобізнаності, є встановлення базової лінії, що визначає рівень знань організації, щоб визначити, де є знання користувачів до та після навчання. Який би підхід не вирішила запровадити організація, важливо, щоб в організації були встановлені політики та процедури, які забезпечують сучасне навчання, яке проводиться часто та має підтримку всієї організації зверху вниз. Необхідно підтримувати інвестиції в технології для виявлення та припинення цих загроз, але разом з цим ми повинні пам'ятати та зосередитися на нашій найслабшій ланці, якою є користувач.

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Кіріл БЛУДОВ

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ ОРГАНІЗАЦІЯМИ ДЛЯ ПІДВИЩЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ

Оскільки технології продовжують розвиватися, кожен штат має забезпечити безпеку, чесність та ефективність своїх поліцейських у своїй роботі. Правоохоронні органи знаходяться на правильному шляху, співпрацюючи з Міністерством юстиції для впровадження політики та програм, які забезпечують безпеку та відповідальність їхніх офіцерів. Окрім безпеки та підзвітності, більше агенцій мають працювати над

впровадженням контролю, коли справа доходить до камер. Немає потреби в технології, щоб зафіксувати телефонний дзвінок дітям або навіть офіцеру, який користується туалетом. Оскільки технології продовжують розвиватися та вносити прогресивні зміни, ми впевнені, що впровадження доступу та контролю в натільних камер можна ефективно зробити, щоб збільшити переваги та зменшити недоліки технологій у правоохоронних органах.

Ми не можемо говорити лише про натільні камери, якими користуються сучасні поліцейські. Слід зазначити, що існує ряд інших технологій, які допомагають у роботі поліції. Ось деякі з них:

Хмарні обчислення.

Як відомо, інформація є ключовою в поліцейській діяльності. Щоб добре виконувати свою роботу, вам потрібен доступ до політик, процедур та інших важливих документів і документів. Хмарні обчислення роблять це можливим. Звіт платформи PowerDMS за 2017 рік про стан політики в правоохоронній сфері показав, що правоохоронні органи посилають нові політики та зміни в електронному вигляді за допомогою хмарного програмного забезпечення для керування політикою. Ця зміна відповідає підвищеному попиту громад на відповідальність, і агенції розглядають це як спосіб захистити себе та свою репутацію. Уже минули ті часи, коли перебирали картотеки та переглядали документи. Хмара дозволяє поліції швидко та зручно отримувати доступ та аналізувати дані кількома способами.

Збір даних та аналіз злочинів.

Швидке відстеження та аналіз великих обсягів даних є важливим для правоохоронних органів, щоб ефективно виконувати свою роботу. За допомогою хмарних обчислень поліція може отримати доступ до точної статистики та інформаційних панелей у режимі реального часу, які відстежують цілі міста. Вони також мають можливість підключати агентства до централізації баз даних кримінального правосуддя. Це може привести до кращої інформації та прийняття рішень.

Управління документами та записами.

Так само програмне забезпечення для керування документами може заощадити офіцерам багато часу. Якщо ви розмістите свої правила та процедури в хмарі, а не в офісі, вони доступні в будь-який час і з будь-якого місця. Це означає, що ваша команда може отримати важливу інформацію, коли це найважливіше. Зберігання документів і записів у хмарі також може заощадити гроші на друку, папері та документації, тож ви можете витратити свої ресурси на покращення своєї спільноти.

Онлайн навчання.

Онлайн-навчання є ще одним важливим інструментом підтримки офіцерів. Одна справа – мати доступ до даних та інших документів. Але

лише тоді, коли ваша команда збереже цю інформацію, вона буде успішною. Ось чому навчання має вирішальне значення. Онлайн-навчання може доповнити особисте практичне навчання, дозволяючи офіцерам зручно та швидко навчатися. Це може заощадити багато грошей і часу, дозволяючи вашим офіцерам бути на полі якомога більше.

Поліцейські повинні отримувати підтримку, інструменти, навчання та компенсацію, які вони потребують і заслуговують, щоб вони могли залишатися в безпеці, захищаючи наші спільноти.

*Консультант з мови **В. В. Кочина***

УДК 351.74:001.895](100)(06)

Яна БОГДАНЕЦЬ

Харківський національний університет внутрішніх справ

ЯК ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ДОПОМАГАЄ В РОЗКРИТТІ ЗЛОЧИНІВ

Штучний інтелект повільно, але впевнено стає дієвим засобом покарання злочинців, а також служить для перевірки протиправних дій. Багато правоохоронних органів у всьому світі використовують найсучаснішу техніку для запобігання злочинам. Штучний інтелект у поліційній діяльності – це система, яка оцінюється за допомогою комп'ютерів. Його також можна використовувати для прийняття рішень, особливо остаточних. Це технологія, яка має великі перспективи для майбутнього в розкритті злочинів.

Тепловізор, який особливо корисний у темряві, став важливим технологічним приладом поліціантів. Тепловізійні камери у вигляді невеликих ручних пристроїв використовують інфрачервоне зображення для виявлення тепла, що випромінюється такими об'єктами, як люди та тварини, і для надання «теплого зображення» або «теплової карти» навколишнього середовища.

Його можна використовувати для відстеження руху підозрюваних у затемненій будівлі. Така технологія застосовується для рятування життя – під час гасіння пожежі або пошуково-рятувальних операцій (наприклад, пошук зниклої дитини чи літньої людини під час хуртовини, коли нічого не видно).

Постійне розширення Інтернету речей (IP) означає, що генерується, збирається та аналізується більше даних, ніж раніше, велика частина яких може бути неймовірно цінною для правоохоронних органів.

Але процес отримання практичних висновків із величезної кількості даних займає настільки неймовірно багато часу, що не є рентабельним, коли це виконують люди. Ось тут на допомогу приходять штучний інтелект (ШІ) і його підкатегорія машинного навчання. ШІ використовується для підтримки багатьох інших поліцейських технологій, зокрема ShotSpotter, для розпізнавання обличчя та біометричних даних.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Олександра БОРИСЮК

Харківський національний університет внутрішніх справ

БПЛА ДЛЯ ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ ТА ПРАВОПОРЯДКУ

Використання правоохоронними органами сучасних технологій відкриває нові можливості для забезпечення безпеки громадян. Впровадження нових технологій у поліцейську діяльність зумовлене в основному необхідністю протистояти злочинному світу, який стає все більш озброєним.

У ХХІ столітті дрони використовуються поліцейськими підрозділами в багатьох країнах світу. Безпілотники надали правоохоронним органам нові можливості, а саме: для спостереження, координації оперативних заходів, аналізу ситуації, пошуків порушників і потерпілих. На озброєнні поліції знаходяться як компактні, готові до польоту квадрокоптери, так і складні багатофункціональні безпілотні системи. Обладнання, якими можуть бути оснащені ці пристрої, забезпечують виконання таких завдань з повітря незалежно від часу доби та погодних умов: патрулювання та спостереження великих територій, пошук і відстеження людей за допомогою тепловізорів, контроль за дотриманням вимог під час масових заходів, моніторинг та аналіз дорожньо-транспортної обстановки та місць ДТП, координація дій поліції.

Використання безпілотних літальних апаратів (БПЛА) має ряд переваг для поліції. Двигуни дронів не видають багато шуму і не заважають громадянам своїм шумом під час масових заходів. У містах з багатоповерховою забудовою поліцейські гелікоптери обмежені у висоті та маневреності. Безпілотник не тільки вільно літає між будівлями, але також може злітати безпосередньо з місць у межах населеного пункту. Час розгортання квадрокоптера становить кілька хвилин, він

поміщається в багажник автомобіля і завжди готовий до використання в інтересах поліції. Дрони вимагають мінімум спеціальних знань. Оновлене програмне забезпечення доступне кожному користувачеві комп'ютера. Такі елементи корисного навантаження, як камери, тепловізори, ліхтарі та динаміки, можна встановити за лічені хвилини. Дрони можуть бути розгорнуті в будь-якому відділі, вони вирішують проблеми з мінімальними експлуатаційними витратами, швидко, безпечно і непомітно.

Науковий керівник Г. М. Сорокіна

УДК [811.111:351.74(100)](06)

Яна БОРЩОВА

Харківський національний університет внутрішніх справ

КІБЕРЗЛОЧИННІСТЬ: СТАРІ ЗЛОЧИНИ ПО-НОВОМУ

Що таке кіберзлочинність? В Австралії термін «кіберзлочинність» використовується для опису обох:

злочини, спрямовані проти комп'ютерів або інших інформаційно-комунікаційних технологій (ІКТ) (такі як комп'ютерні вторгнення та атаки відмови в обслуговуванні), а також

злочини, коли комп'ютери або ІКТ є невідомою частиною злочину (наприклад, шахрайство в Інтернеті)

Так само, як Інтернет та інші нові технології відкривають величезні можливості, вони також дають можливість злочинцям вчиняти нові злочини та вчиняти старі злочини по-новому. З наявних доказів стає ясно, що кількість, складність і вплив кіберзлочинів продовжують зростати і становлять серйозну загрозу для окремих осіб, підприємств та урядів Австралії.

Злочинці в Інтернеті можуть миттєво вчиняти злочини через декілька кордонів і одночасно націлюватися на велику кількість жертв. Інструменти, які мають багато законних застосувань, як-от високошвидкісний Інтернет, одноранговий обмін файлами та складні методи шифрування, також можуть допомогти злочинцям здійснювати та приховувати свою діяльність.

AFP відповідає за виявлення, запобігання, порушення, реагування на кіберзлочини, що впливають на всю австралійську економіку, та забезпечення їх виконання. Він зосереджений на розслідуванні загроз кіберзлочинності проти відомств уряду Співдружності, критичної інфраструктури та інформаційних систем національного значення,

ключовим елементом яких є банківський та фінансовий сектор. АФР керується пріоритетами Співдружності щодо боротьби з кіберзлочинністю.

Загалом розслідування шахрайства щодо фізичної особи є обов'язком державної поліції. Однак там, де є перехід між розслідуванням шахрайства проти фізичної особи та розслідуванням організованої атаки на критично важливі банківські системи, АФР працюватиме разом із місцевою юрисдикцією та банківською та фінансовою галуззю. АФР також тісно співпрацює з поліцією штатів і території та міжнародними поліцейськими агентствами у боротьбі з усіма видами кіберзлочинності.

Тим не менш, найкращим способом боротьби з кіберзагрозами є забезпечення того, щоб ви розуміли та використовували належну кібербезпеку. Найпростіший спосіб залишатися в курсі, якщо це можливо, увімкнути або підтвердити автоматичні оновлення. Автоматичне оновлення – це функція «встановити і забути», яка оновлює ваше програмне забезпечення, щойно воно стає доступним.

Мовний радник І. О. Гоголь

УДК [811.111:351.74(100)](06)

Олександр БУЛИШ

Харківський національний університет внутрішніх справ

ТЕХНОЛОГІЇ, ЯКІ ДОПОМОГАЮТЬ ПІДВИЩИТИ БОРОТЬБУ ЗІ ЗЛОЧИННІСТЮ

З посиланням на Університет Пейс, технології допомагають правоохоронним органам і працівникам юстиції залишатися на крок попереду злочинців, надаючи нові способи виявлення та запобігання злочинам, а також допомагаючи прокурорам засуджувати правопорушників. А оскільки нові технології доступні по обидва боки правосуддя, гра в кішки-мишки між злочинцями та поліцією не закінчується, і правоохоронні органи потребують постійних коригувань. Доброю новиною для громадської безпеки є те, що рівень злочинності загалом знизився за останні два десятиліття, частково завдяки прогресу в розкритті злочинів і технології стримування. Оскільки ефективна поліція значною мірою спирається на швидкий обмін конфіденційними даними про злочини; недавній вибух інформаційних технологій є позитивним зрушенням для правоохоронних органів. Технологія ідентифікації, соціальні медіа та мобільні можливості також підвищують громадську безпеку, дозволяючи працівникам правосуддя вести свою справу більш ефективно та реагувати на розгортаються розслідування в режимі реального часу.

Хоча технології ставлять проблеми для правоохоронних органів, які постійно намагаються не відставати від технологічних злочинних підприємств; він приносить більше користі, ніж шкоди в боротьбі зі злочинністю. Технічні досягнення в правоохоронних органах включають наступні можливості, які ілюструють, як швидко все змінюється разом із технологіями.

Обмін інформацією – правоохоронні органи розповсюджені по всій національній системі кримінального правосуддя, до якої входять регіональні, державні та місцеві органи влади, кожен з яких самостійно керує своїми поліцейськими зусиллями. Обмін інформацією про правопорушників також має позитивний превентивний вплив, допомагаючи утримувати зброю від рук небезпечних злочинців і забороняючи правопорушникам певні види роботи.

Покращення системи безпеки та відеоспостереження – злочини проти власності продовжують статистично зменшуватися, тому оновлення системи безпеки та відеоспостереження значно покращило громадську безпеку.

Соціальні медіа – хоча це соціальна тенденція настільки, наскільки це технологічний прорив, використання соціальних медіа, тим не менш, надає переваги правоохоронним органам для агентств, які ефективно використовують цю технологію.

Технологія картографування злочинності – сучасні обчислювальні потужності прискорюють аналіз даних і дають правоохоронним органам змогу відстежувати тенденції злочинності в географічному відношенні.

Мобільна технологія – мобільна технологія забезпечує електронний слід із текстів, електронних листів, дзвінків та інформації про місцезнаходження GPS, яку правоохоронні органи використовують для розкриття справ. Смартфони настільки широко поширені, що контактна інформація та інші дані, які вони містять, дають офіцерам відправну точку для їх розслідувань, які часто розгортаються під час арештів, безпосередньо пов'язаних з інформацією, отриманою з мобільних пристроїв та використанням.

Технології ніколи не замінять серйозну слідчу роботу, але сучасні досягнення допомагають правоохоронним органам триматися попереду злочинців. Мобільні технології, соціальні мережі та швидкий доступ до інформації сприяють кращому запровадженню та запобіганню. Прориви в картографуванні злочинності та відеоспостереження також підвищують громадську безпеку, дозволяючи органам юстиції спрямовувати ресурси туди, де вони найбільше потрібні.

Мовний консультант І. О. Гоголь

УДК 351.74:001.895](100)(06)

Софія ВАСИЛЬЧЕНКО

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ СИСТЕМИ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ТРАНСПОРТНИХ ЗАСОБІВ

Букви та цифри на номерних знаках автомобілів допомагають правоохоронцям визначити викрадені транспортні засоби, чи власників, що розшукуються. Нові технології спрощують цей процес. Система автоматичного розпізнавання номерних знаків (САРНЗ) є інтегрованою технологією камери-базис даних в якій система фотографує номерний знак автомобіля, а потім обробляє цифри та літери у відомій базі даних, попереджаючи поліціанта про підозрілість автомобіля.

САРНЗ може, з більшою точністю та без фактору втоми, ідентифікувати, перевіряти та записувати номерні знаки більшої кількості транспортних засобів, ніж такої, з якою може впоратися цілий загін поліціантів. Це означає, що більше розшукваних транспортних засобів затримується за меншу кількість часу, що робить цю технологію для правоохоронних органів такою, без якої зараз жоден поліціант не хоче обходитися.

САРНЗ використовує комбінацію камер і комп'ютерного програмного забезпечення, щоб без розбору сканувати номерні знаки кожного автомобіля, що проходить повз. Зчитувачі, які можна встановити на стаціонарних стовпах, рухомих поліцейських патрульних автомобілях і, навіть, портативних пристроях, записують час і дату кожного сканування, ГСП-координати транспортного засобу та фотографії автомобіля. Деякі версії також можуть фотографувати пасажирів автомобіля та створювати унікальні ідентифікатори транспортних засобів.

Пристрої надсилають дані до програмного забезпечення САРНЗ, яке може порівняти кожний запис з визначеним «гарячим списком». Такі списки можуть включати викрадені автомобілі та автомобілі, пов'язані з системою оповіщення «Ембер» про викрадених дітей. Вони також можуть визначати транспортні засоби, які вказані в місцевих та федеральних базах даних з причин, які можуть включати неоплачені штрафи за паркування або наявність в базі даних банд. Ці запити відбуваються автоматично, хоча поліціанти також можуть запитувати номерні знаки вручну.

Окрім перевірки даних у режимі реального часу, багато міст та агенцій зберігають інформацію про номери для подальшого використання, іноді на невизначений термін. Ці дані можна

використовувати для визначення різних місць розташування конкретного транспортного засобу або для ідентифікації всіх автомобілів у певному місці, а також їх навіть можна проаналізувати, щоб передбачити маршрути та майбутнє розташування одного транспортного засобу, чи одразу декількох транспортних засобів.

Для правоохоронних органів було практично неможливо регулярно стежити за всіма водіями. Однак із зростаючим використанням САРНЗ, поліція тепер може отримувати інформацію про рух автомобіля в режимі реального часу та переглядати минулі пересування одним натисканням кнопки.

*Науковий керівник **Олександр Олішевський***

УДК [351.74: 001.895(100)](06)

Вадим ВЛАСОВ

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Важливу роль у діяльності правоохоронних органів, відіграє злочинність. Боротьба зі злочинністю ведеться в усіх країнах, різними державними організаціями, підприємствами, громадянами. Запобігати злочинам потрібно на початковому етапі, коли злочинець тільки замишляє та планує вчинення певного діяння.

На сьогоднішній день, ефективність діяльності правоохоронних органів, залежить від технічного оснащення. Якщо бути точнішим, в практичну діяльність органів Національної поліції України, широко впроваджується злічувальна техніка, автоматизовані робочі місця, які обладнані сучасними персональними комп'ютерами та великою базою даних. Це допомагає практичним працівникам, вони менше виконують одноманітну роботу, тобто вся праця покладена на технічне оснащення. Сьогодні, технології допомагають знаходити рішення при розв'язанні різноманітних питань, дають можливість ширше вивчати процеси, розібрати їх.

В умовах зростаючої комп'ютеризації, у тому числі і в Національній поліції України, головною метою процесу розвитку, є надання курсантам, студентам та слухачам закладів вищої освіти МВС України, працівникам органів Національної поліції спеціальних знань, умінь та навичок з іноваційних технологій та інформаційного забезпечення їх професійної діяльності, які ефективно використовують комп'ютерну техніку та сучасні інформаційні технології у своїй оперативно-службовій діяльності.

Функція миттєвого чату є важливим інструментом для спілкування в режимі реального часу з хворими пацієнтами або пацієнтами в масках, а також глухими. А служби визначення місцезнаходження засновані на місцезнаходження пристрою абонента, що дозволяє точно визначити, де перебуває особа. Незважаючи на те, що для стеження за людьми необхідно мати спеціальний дозвіл від відповідних установ, існує не менше трьох способів, як можна дізнатися місце розташування людини за його номером телефону. Це буває необхідно, коли потрібно знайти дитину, що загубилась або злочинця, що в пошуку. Пошук людей за номером телефону можливий через спеціалізовані програми. Ці знання потрібно покращувати і розвивати через інформаційні технології.

Коли вдарив COVID, багато офіцерів зрозуміли, що функції миттєвого чату також допомагають їм зменшити потребу в особистих зустрічах для рутинної роботи поліції, яку можна було б виконувати по телефону.

Хоча ці технології були створені або вдосконалені, щоб допомогти правоохоронним органам адаптуватися до умов, що змінюються через пандемію COVID-19, багато з цих проблем існували до пандемії і продовжуватимуть існувати, коли світ пристосовується до нової норми.

Спрощені процеси призведуть до більшої безпеки для співробітників правоохоронних органів і людей, яких вони обслуговують, потрібно покращити обізнаність у сфері іноваційних технологій, тоді покращиться точність визначення місцезнаходження, швидше почнуть розвиватись функції миттєвого чату, більше автоматизувати робочі місця, які обладнані сучасними персональними комп'ютерами та великою базою даних, тоді зросте довіра населення до правоохоронних органів, а це головне.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Вікторія ГОРДУСЕНКО

Харківський національний університет внутрішніх справ

ШАХРАЙСТВО З КРЕДИТНИМИ КАРТКАМИ

Половина всього шахрайства з кредитними картками починається зі шпигунського програмного забезпечення, шкідливого програмного забезпечення, несвідомо встановленого на комп'ютері або портативному пристрої жертви. Шпигунське програмне забезпечення працює у фоновому режимі, збирає ваші дані та надсилає їх злочинцю, який потім використовує вашу картку для здійснення шахрайських покупок.

Шахрайство з кредитними картками – це несанкціоноване використання кредитної чи дебетової картки чи подібного платіжного інструменту (ACH, EFT, регулярні платежі тощо) для шахрайського отримання грошей чи майна. Номери кредитних і дебетових карток можна вкрасти з незахищених веб-сайтів або отримати за схемою крадіжки особистих даних. Шахрайство з кредитною картою – це включний термін для шахрайства, скоєного за допомогою платіжної картки, наприклад кредитної або дебетової картки. Метою може бути отримання товарів чи послуг або здійснення платежу на інший рахунок, який контролюється злочинцем. Стандарт безпеки даних індустрії платіжних карток (PCI DSS) – це стандарт безпеки даних, створений, щоб допомогти фінансовим установам безпечно обробляти карткові платежі та зменшити шахрайство з картками. Шахрайство з кредитною картою може бути авторизованим, коли справжній клієнт самостійно обробляє платіж на інший рахунок, який контролює злочинець, або неавторизованим, коли власник рахунку не надає авторизацію для здійснення платежу, а транзакція здійснюється третьою стороною. Кредитні картки безпечніші, ніж будь-коли, оскільки регулятори, постачальники карток і банки витрачають багато часу та зусиль на співпрацю зі слідчими по всьому світу, щоб переконатися, що шахраї не досягнуть успіху. Гроші власників карток зазвичай захищені від шахраїв за допомогою правил, які зобов'язують постачальника карток і банк підзвітні. Технології та заходи безпеки кредитних карток стають дедалі складнішими, що ускладнює крадіжку грошей шахраям.

Є два види шахрайства з картками: шахрайство з картою (нині не так часто) і шахрайство без картки (частіше). Компроміс може відбуватися кількома способами і зазвичай може відбуватися без відома власника картки. Інтернет зробив проблеми безпеки баз даних особливо дорогими, у деяких випадках мільйони облікових записів були скомпрометовані. Власники карток можуть швидко повідомити про викрадені картки, але дані про зламаний обліковий запис можуть зберігатися у шахрая місяцями до будь-якої крадіжки, що ускладнює визначення джерела компромісу. Власник картки не може виявити шахрайське використання, доки не отримає виписку. Власники карток можуть зменшити цей ризик шахрайства, часто перевіряючи свій рахунок, щоб переконатися, що немає підозрілих або невідомих транзакцій. У разі втрати або крадіжки кредитної картки її можна використовувати для незаконних покупок, поки власник не повідомить банк-емітент і банк не заблокує рахунок. Більшість банків мають безкоштовні цілодобові номери телефонів, щоб заохочувати оперативну звітність. Тим не менш, злодій може зробити несанкціоновані покупки на картці до її анулювання.

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Максим ГУНЬКО

Харківський національний університет внутрішніх справ

БЕЗПЕРЕРВНИЙ РОЗВИТОК ТЕХНОЛОГІЙ ПРАВООХОРОННИХ ОРГАНІВ

Розвиток інформаційних технологій дозволить зберігати будь-яку інформацію, яка стосується конфіденційності, і, якщо це потрібно, поширювати її в електронному вигляді всіма органами кримінального правосуддя. Це піде на користь правоохоронним органам та поліції в прокуратурі, а також захисникам як приватних, так і державних адвокатів. Сьогодні ця мета вже почала реалізовуватися. Однак ефективна інформаційна система, що використовує цю технологію, має бути добре скоординована та спланована між відповідними органами, щоб уникнути виникнення технологічних невідповідностей. При належному плануванні поліція може тісно співпрацювати з членами громади, щоб зменшити злочинність, а також створити більш безпечну спільноту. Ця технологія зведе до мінімуму адміністративні ролі людини і водночас підвищить ефективність управління, а також підзвітність усіх офіцерів. У майбутньому міські органи легко визначать та нададуть рішення проблем сусідства замість того, щоб реагувати на злочин ще довго після його скоєння. Мета буде легко досягнута шляхом широкого навчання, щоб допомогти громадянам, а також поліцейським оволодіти вбивствами при використанні послуг, що впливають на злочинність, а також методів націлювання на гарячі точки для злочинної діяльності.

Правоохоронці також стикалися з великим попитом на обмін даними з іншими агентствами та підприємствами, включаючи страхові компанії. Розвиток технологій також був спрямований на покращення управління поліцією, а також на її підзвітність щодо доброчесності. Технологія зробила витрати на розслідування злочинів ефективними в результаті дотримання регулярних процедур. Були розроблені різні методи, щоб вчасно попередити поліцію про застосування сили. Завдяки новітнім технологіям поліція ретельно перевіряється через внутрішні системи управління наглядовими та наглядовими агенціями.

Таким чином, правоохоронні технології спрямовані на охорону як громадян, так і поліцейських, щоб змусити їх покращити свої служби, особливо в карті злочинності, а також інтеграції інформації. Прикладом застосування технології з 1990 року є комп'ютерне картування злочинності, яке використовувалося як інструмент правоохоронними органами. Географічна інформаційна система була об'єднана з

програмним забезпеченням для картографування та використовувалася з настільними комп'ютерами для аналізу злочинності. Дослідження показують, що ця технологія доступна навіть для підрозділів поліції, які працюють з обмеженим бюджетом.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Вадим ГУЦАЛ

Харківський національний університет внутрішніх справ

МАЙБУТНЄ ПРАВОВОГО ВРЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ

Оскільки новітні технології стимулюють нові моделі бізнесу та послуг, уряди повинні швидко створювати, змінювати та запроваджувати правила. Головне питання полягає в тому, як захистити громадян і забезпечити справедливі ринки, дозволяючи інноваціям і бізнесу процвітати. Стрімкі технологічні досягнення вносять серйозні зміни в сучасне регуляторне середовище, створюючи значні проблеми для регуляторів, які прагнуть підтримувати баланс між стимулюванням інновацій, захистом споживачів і подоланням потенційних ненавмисних наслідків порушення.

Нові технології, такі як штучний інтелект (ШІ), машинне навчання, аналітика великих даних, технологія розподіленої книги та Інтернет речей (IoT), створюють нові способи взаємодії споживачів і руйнують традиційні бізнес-моделі. Це епоха, коли машини вчать вчитися самі; автономні транспортні засоби зв'язуються один з одним і транспортною інфраструктурою; а розумні пристрої відповідають і передбачають потреби споживачів.

Після цих подій перед керівниками регуляторних органів постає ключове завдання: як найкраще захистити громадян, забезпечити справедливі ринки та забезпечити дотримання правил, дозволяючи цим новим технологіям і бізнесу процвітати? Припущення про те, що нормативні акти можна розробляти повільно й свідомо, а потім залишатися в силі, незмінними, протягом тривалого періоду часу, було скасовано в сучасних умовах. Оскільки з'являються нові бізнес-моделі та послуги, такі як послуги спільного користування та первинні пропозиції монет, державні установи стикаються зі створенням або зміною нормативних актів, їх дотриманням та інформуванням громадськості в непередбачуваному раніше темпі. І вони повинні робити це, працюючи в застарілих рамках та намагаючись сприяти інноваціям.

Сьогодні регулятори стикаються з подібними проблемами. Вони повинні збалансувати свої обов'язки щодо захисту громадян із просуванням інновацій у нових технологіях та бізнесі, протистояти потягу до надмірного регулювання. Для технологічних інновацій регулювання може бути як каталізатором, так і перешкодою. Оскільки нові технології розвиваються, регулятори з усього світу переосмислюють свої підходи, приймаючи моделі, які є гнучкими, ітеративними та спільними, щоб протистояти викликам, що виникають через нові технології та четверту промислову революцію. Щоб заохочувати інновації, регулятори також рухаються до створення нормативних актів, що ґрунтуються на результатах, та тестування нових моделей у пісочницях.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Олександр ДАВИДОВ

Харківський національний університет внутрішніх справ

ОЦИФРОВКА РОБОТИ ПОЛІЦІЇ

Модернізація криміналістики йде вперед. З'являються нові методики, засоби знаходження та фіксування слідів на місці злочину, спеціальні пристрої та обладнання. Технології вдосконалюються з року в рік. Використання правоохоронними органами сучасних технологій відкриває нові шляхи забезпечення безпеки громадян. Сучасні інформаційно-комунікаційні технології підкорили наше повсякденне життя, зробивши його ефективнішим, результативнішим, гнучкішим і динамічнішим.

«Людина, яка використовує сучасні технології, відкидає цифрову тінь». Вона створюється з урахуванням всієї інформації, яку користувач залишає в Інтернеті – так званих метаданих. Технологіями великих даних користуються правоохоронні органи для моніторингу соціальних процесів у суспільстві, прогнозування та запобігання злочинності. Сюди входить криміналістичне дослідження інформації з мобільних пристроїв: даних про вхідні та вихідні дзвінки, контакти, отримані та надіслані повідомлення, у тому числі тих, що містяться в зашифрованому чи прихованому вигляді тощо.

Впровадження цифрових технологій у діяльність поліції значною мірою зумовлено необхідністю протистояти все більш озброєному кримінальному світу. Злочинці активно користуються останніми досягненнями четвертої промислової революції. Наслідки злочинів, які необхідно враховувати у діяльності поліції, стають дедалі ширшими та серйознішими.

Більшість злочинів розкриваються за допомогою систем відеоспостереження. На даний момент всюди працюють відеокамери, дані з яких збираються в «Єдиному центрі зберігання та обробки даних». Записи камер відеоспостереження можуть бути використані як цінний матеріал у кримінальному провадженні. Зараз поліція активно використовує дрони. Оснащені відеокамерою, вони використовуються там, де поліцейському може загрожувати небезпека. Безпілотники також можуть брати участь у переслідуванні злочинців.

Оцифровка роботи поліції є динамічним процесом. Найсучасніші технології є незамінними для поліції в цифровому світі. Використання цих технологій дає змогу поліції ефективніше виконувати свої завдання та підвищувати довіру громадян.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Катерина ДАЦЕНКО

Харківський національний університет внутрішніх справ

КРИПТОДЖЕКІНГ ЯК СУЧАСНА ГОТІВКА

Криптоджекінг — це тип кіберзлочинів, коли злочинець таємно використовує обчислювальні потужності жертви для створення криптовалюти. Основні наслідки криптоджекінгу включають: уповільнення роботи пристрою; перегрів батарей; підвищене споживання енергії; пристрої виходять з ладу; і зниження продуктивності. Криптоджекінг в хмарі також може призвести до додаткових витрат для компаній, які виставляються на основі використання ЦП.

Криптоджекінг (також званий зловмисним криптомайнінгом) — це онлайн-загроза, яка ховається на комп'ютері або мобільному пристрої та використовує ресурси машини для «добування» форм онлайн-валюти, відомих як криптовалюти. Шкідливі криптомайнери часто надходять через завантаження веб-браузера або шахрайські мобільні програми. Криптоджекінг може пошкодити всі види пристроїв, включаючи настільні комп'ютери, ноутбуки, смартфони і навіть мережеві сервери. Як і більшість інших зловмисних атак на комп'ютерну громадськість, мотивом є прибуток, але на відміну від багатьох загроз, він розроблений так, щоб залишатися повністю прихованим від користувача. Щоб зрозуміти механізм загрози та як захиститися від неї, давайте почнемо з невеликої інформації.

Криптовалюти — це форми цифрових грошей, які існують лише в онлайн-світі, без реальної фізичної форми. Вони були створені як

альтернатива традиційним грошам і здобули популярність завдяки своєму перспективному дизайну, потенціалу зростання та анонімності. Одна з найперших, найуспішніших форм криптовалюти, біткойн, з'явилася в 2009 році, а в наступні роки отримала широке визнання. Успіх біткойна надихнув десятки інших криптовалют, які працюють більш-менш так само. Можливо, вам знайомі, наприклад, такі імена, як Ethereum або Dogecoin. Сьогодні люди в усьому світі використовують криптовалюту, щоб купувати речі, продавати речі та робити інвестиції. Два слова — «криптографія» і «валюта» — поєднуються, утворюючи «криптовалюту», тобто електронні гроші, засновані на принципах складного математичного шифрування. Усі криптовалюти існують як зашифровані децентралізовані грошові одиниці, які вільно передаються між учасниками мережі. Або простіше кажучи, криптовалюта — це електроенергія, перетворена в рядки коду, які мають реальну грошову вартість.

Незалежно від того, чи були ви заблоковані локально у вашій системі чи через браузер, може бути важко вручну виявити вторгнення після факту. Аналогічно, знайти причину високого використання ЦП може бути важко. Процеси можуть ховатися або маскуватися як щось законне, щоб перешкодити вам зупинити зловживання. Як бонус для срутjockers, коли ваш комп'ютер працює на максимальній потужності, він працюватиме надповільно, і, отже, його буде складніше усунути. Як і з усіма іншими застереженнями щодо шкідливого програмного забезпечення, набагато краще встановити безпеку, перш ніж стати жертвою.

*Консультант з мови **В. В. Кочина***

УДК 351.74:001.895](100)(06)

Олександр ДЖИГА

Харківський національний університет внутрішніх справ

НОВІ МЕТОДИ ТРИВИМІРНОГО ДОКУМЕНТУВАННЯ МІСЦЯ ЗЛОЧИНУ

Багато вчених працюють над розробкою нових методів і засобів розкриття злочинів. Робота слідчих на місці події після вчинення злочину має велике значення, але лише незначна частина співробітників поліції, які працюють над розслідуванням, перебувають безпосередньо на місці злочину та фіксують докази. Багато з них знайомляться з картиною події лише пізніше. В цьому дуже допомагає спеціальне обладнання.

Останнім досягненням є 360-градусна камера Spheron, яка використовується для зйомки місця злочину. Пристрій пропонує роздільну здатність 50 мільйонів пікселів і 400-кратний зум. Він надає можливість відображати найдрібніші деталі в затемнених приміщеннях так само яскраво, як вдень, і документувати місце злочину у вигляді повної тривимірної моделі. Просте та швидке отримання зображення за допомогою 360-градусної фотографії – один із способів значно підвищити точність документування місця злочину за рахунок використання цієї технології. Такі 3D-моделі використовуються як засіб довгострокового і повного збереження просторової обстановки на місці злочину.

В інтерв'ю Мехзеб Чоудхурі, доктор наук у галузі криміналістики та криміналістичних досліджень Даремського університету, пояснив проблеми, пов'язані з порушенням місця події та особистими відвідуваннями: «Найбільш проблематичним аспектом відвідувань місця злочину є те, що з часом кожна характеристика місця події певним чином змінюється. Це називається порушенням місця події. Одночасна зйомка всього місця злочину дозволила б зберегти необхідні деталі для розслідування та судового процесу». Ті, хто ніколи не був на місці злочину, зможуть отримати справжню картину події в будь-який момент. Завдяки цій технології інформація доступна в більш реалістичній формі.

Технології вже давно відіграють важливу роль у правоохоронній діяльності. І тепер, з розвитком 360-градусної фотографії та віртуальної реальності, відтворення місця злочину стало більш точним, ніж будь-коли. 3D-моделі, створені на місці злочину, покликані допомогти у розумінні просторового розташування слідів під час судового засідання та надати базу даних для наочної ілюстрації справи. Крім того, вони сприяють як об'єктивності судді щодо доказів, так і юридичної визначеності для засудженої особи.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Назар ДОБРОЗНАЙ

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ (БПАС) У РОБОТІ ПОЛІЦІЇ

Якщо ви думали, що роботи з камерами з дистанційним керуванням - це круто, ви будете вражені почути, що деякі правоохоронні органи експериментували з використанням безпілотних

авіаційних систем (БПЛА), іноді відомих як дрони. БАС можна використовувати для пошуку підозрюваних, отримання інформації та обстеження районів надзвичайних ситуацій без використання пілотованого гелікоптера або літака. Технологія БПЛА не тільки може заощадити гроші, але також може захистити співробітників правоохоронних органів від шкоди.

Кількість безпілотників постійно зростає, і органам авіаційного руху терміново потрібні рішення для управління їх присутністю в повітряному просторі, як і будь-яких інших типів літаків.

Враховуючи специфічні характеристики роботи БАС, вони повинні бути такими ж безпечними, як і пілотовані. Технології для безпілотних літальних апаратів дозволяють виконувати широкий спектр можливих операцій. Для забезпечення безпеки людей на землі та інших користувачів повітряного простору під час експлуатації безпілотних літальних апаратів повинні бути встановлені вимоги щодо льотної придатності, організації та осіб, залучених до експлуатації БПЛА, та безпілотних літальних апаратів. Правила та процедури, що застосовуються до роботи БАС, повинні бути пропорційними характеру та ризику операції чи діяльності та адаптованими до експлуатаційних характеристик відповідного безпілотного повітряного судна та характеристик району виконання операцій, таких як щільність населення, характеристики земної поверхні та наявність будівель. Критерії рівня ризику, а також інші критерії, слід використовувати для встановлення трьох категорій операцій: категорії «відкриті», «специфічні» та «сертифіковані».

Правоохоронні органи можуть використовувати дрони для ефективнішої роботи поліції і використовувати їх для збору доказів і проведення спостереження, для фотографування місць дорожньо-транспортних пригод, моніторингу виправних установ, відстеження втікачів із в'язниці, відстеження підозрюваних, відшукування зниклих осіб, фотографування місць скоєння злочину, контролю натовпу тощо. Якщо впроваджувати та використовувати дрони обережно, вони можуть стати величезним здобутком для правоохоронних органів. Вони можуть допомогти підрозділам збирати важливу інформацію в небезпечних ситуаціях, заощаджуючи при цьому робочу силу та гроші.

Хоча ця технологія в правоохоронних органах наразі доступна, широке використання безпілотних літальних апаратів розвивається повільно через правила їх застосування та критику з боку громадськості. Чи стануть ці безпілотні літаки масовою частиною наших правоохоронних органів, покаже час.

*Науковий керівник **Олександр Олішевський***

УДК 351.74:001.895](100)(06)

Альона ДОББИШ

Харківський національний університет внутрішніх справ

МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОННІЙ СИСТЕМІ

Безпека є базовою потребою людини. Це забезпечують правоохоронні органи, дорожня поліція та служби безпеки.

Безпека дорожнього руху: наприклад, у Великобританії та Австралії поліція використовує нові вуличні камери для відстеження водіїв, які користуються телефонами під час керування автомобілем. Ця технологія заснована на сенсорних радарних датчиках, які фотографують водіїв через лобове скло.

Спостереження за великими об'єктами: програмне забезпечення у цьому секторі призначене для сфери енергетики, комунальних послуг, електростанцій, водних та атомних станцій. Цифрові засоби безпеки комбінують сейсмічні, бездротові та оптичні датчики з «тепловізорами» та «відеоспостереженням», надаючи повний огляд території, що охороняється. Система спрацьовує при виявленні вторгнення. Сигналізація спрацьовує, якщо транспортний засіб або людина потрапляють у заборонену зону або залишаються там довше, ніж дозволено.

Безпека масових заходів: запобігання заворушень і терористичних атак, гарантування безпеки на концертах чи під час інших великих скупчень людей - для таких завдань також розробляються спеціальні системи з функцією розпізнавання облич. Якщо з'ясовується, що відвідувач представляє інтерес для поліції або інших служб, його фото та особисті дані відображаються на планшеті співробітника служби безпеки та відзначаються червоним кольором.

Спостереження за приватними будинками та квартирами: системи безпеки житла на основі штучного інтелекту є найсучаснішим способом охорони приватних будинків та квартир. Така система здатна розпізнавати обличчя, предмети та фігури людей. Якщо обличчя не розпізнається штучним інтелектом протягом 20 секунд, вмикається сирена і здійснюється екстрений виклик поліції.

Який підсумок? - Інтелектуальні системи безпеки, якими керують поліцейські командні центри, ефективні для спостереження, попередження злочинності та запобігання терористичних нападів. Використання таких систем дисциплінує суспільство та підвищує громадську безпеку.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Віталій ДОНЧЕНКО

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ШВИДКІСНИХ РАДАРІВ НА ДОРОГАХ УКРАЇНИ

Останнім часом в Україні зростає кількість ДТП через перевищення швидкості. Враховуючи цей факт, Національна поліція України вирішила протидіяти цим злочинам за допомогою високошвидкісних радарів Trusam на дорогах, які широко використовуються поліцією Німеччини.

У Німеччині порушення фіксують 3500 стаціонарних радарів, які встановлені як на трасах, так і в населених пунктах. Про контроль і нагляд водіїв сповіщає табло з написом «Радарконтроль».

В Україні кількість ділянок, на яких вимірюється швидкість за допомогою приладу Trusam, нещодавно зростає до 309. З понеділка, 22 березня 2021 року, патрульні з приладом Trusam розпочали роботу на нових 60 пунктах. Нові місця були обрані на основі аналізу аварій із перевищенням швидкості. Дорожні знаки на таких ділянках повідомлять водіям про фото- та відеофіксацію.

Хоча Україна використовує досвід інших країн у сфері цифрових технологій, які використовуються в роботі правоохоронних органів, у нас все ще бракує ресурсів для роботи в цій сфері. Як правило, не вистачає фінансування з боку держави, не вистачає спеціалістів для роботи з новими технологіями та не ідеальне законодавство. Використання цифрових технологій у роботі правоохоронних органів – це неминуче майбутнє, яке обов'язково допоможе та полегшить роботу поліції, тому держава має приділяти більше уваги питанням, пов'язаним із впровадженням досвіду інших держав у цій сфері.

Консультант з мови: Н. В. Краснова

УДК 351.74:001.895](100)(06)

Кирило ДУЛІН

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ПОРТАТИВНИХ ЛАЗЕРІВ ДЛЯ ДОСЛІДЖЕННЯ МІСЦЯ СКОЄННЯ ЗЛОЧИНУ

Щодня працівники правоохоронних органів стикаються з невідомими підозрілими речовинами, які потребують негайної ідентифікації перед підтвердженням відповідних дій. Коли йдеться про

кримінальні розслідування, немає права на помилку, а попит на швидкі та точні мобільні методи виявлення та ідентифікації вищий, ніж будь-коли. На сьогодні правоохоронні органи використовують портативні лазери для дослідження місця скоєння злочину. Ручні пристрої лазерної спектроскопії можуть визначити хімічний склад невідомої речовини за лічені секунди. Якщо поліціант натрапить на підозрілу речовину, ці пристрої майже відразу виявлять її хімічний склад. Цей тип миттєвої технології правоохоронних органів скорочує час перебування поліціантів в офісі, чи в лабораторії, дозволяючи більше часу на дії. Ці лазери також захищають поліціантів від шкідливих речовин, які вони могли б не впізнати інакше. Велике навантаження на лабораторії призводить до непотрібних затримок з отриманням доказів до суду і впливає на здатність суду призначити заставу для підозрюваного. Ще одним стимулом для використання мобільних технологій виявлення є тривалий час і великі витрати, пов'язані з лабораторними аналітичними методами. У випадку, коли під час аналізу лише незначна частина доказів призводить до судових позовів, використання мобільних технологій виявлення для скринінгу зразків дозволить користувачам визначити ідентичність речовини перед відправкою її в лабораторію для подальшого аналізу. Раманівська спектроскопія є високо селективною технікою і має здатність розрізняти широкий спектр сполук, що є критичним, коли стикаються з все більш широким спектром загроз. На відміну від інших ручних методів виявлення, Раманівський аналіз часто можна виконувати через пакувальний матеріал, не порушуючи зразок. Це мінімізує вплив на них спеціаліста та зменшує ризик забруднення зразка. Захист доказів від забруднення є критичним для успішного передачі справи до суду. Крім того, на відміну від багатьох інших технологій виявлення, які вимагають добре підготовленого спеціаліста для інтерпретації складних результатів, пристрій може використовуватися не підготовленим працівником, який отримає ті ж результати, що й хімік рівня кандидата технічних наук. Дозволяючи користувачам проводити підтверджуючий аналіз після арешту та надавати суттєві, перевірені докази, справи можуть передаватися до суду набагато швидше, допомагаючи скоротити відставання та підвищити рівень успішності видалення небезпечних речовин з обігу.

Науковий керівник Олександр Олішевський

УДК 351.74:001.895](100)(06)

Олексій ЖИЖИРІЙ

Харківський національний університет внутрішніх справ

ЗЛОМ: ВИДИ ТА БЕЗПЕКА

Зазвичай використовується визначення хакерства – це скомпromетація цифрових пристроїв і мереж через несанкціонований доступ до облікового запису або комп'ютерної системи. Злом не завжди є зловмисним актом, але найчастіше він пов'язаний з незаконною діяльністю та крадіжкою даних кіберзлочинцями. Злом — це зловживання такими пристроями, як комп'ютери, смартфони, планшети та мережі, з метою пошкодження систем, збору інформації про користувачів, крадіжки даних і документів або порушення діяльності, пов'язаної з даними. Традиційний погляд на хакерів – це самотній програміст-шахрай, який володіє високою кваліфікацією в кодуванні та модифікації комп'ютерного програмного та апаратного забезпечення. Але цей вузький погляд не охоплює справжню технічну природу злomu. Хакери все більше вдосконалюються, використовуючи приховані методи атак, розроблені так, щоб програмне забезпечення кібербезпеки та ІТ-команди залишалися абсолютно непоміченими. Вони також мають високу кваліфікацію у створенні векторів атак, які обманом змушують користувачів відкривати шкідливі вкладення або посилання та вільно відмовлятися від своїх конфіденційних особистих даних. В результаті сучасний злом передбачає набагато більше, ніж просто розлучену дитину в їхній спальні. Це багатомільярдна індустрія з надзвичайно складними й успішними технологіями.

Зазвичай існують чотири основні чинники, які призводять до злomu веб-сайтів або систем зловмисниками: (1) фінансова вигода через крадіжку даних кредитної картки або шахрайство з фінансовими послугами, (2) корпоративне шпигунство, (3) здобути популярність або повагу до своїх хакерських талантів та (4) злом, спонсорований державою, метою якого є крадіжка бізнес-інформації та національної розвідки. Крім того, є політично мотивовані хакери — або хактивісти — які прагнуть привернути увагу громадськості шляхом витоку конфіденційної інформації, як-от Anonymous, LulzSec та WikiLeaks. Деякі з найпоширеніших типів хакерів, які здійснюють такі дії: Black Nacker Hackers є «поганими хлопцями» на сцені злomu. Вони докладають всіх зусиль, щоб виявити вразливі місця в комп'ютерних системах і програмному забезпеченні, щоб використовувати їх для фінансової вигоди або для більш зловмисних цілей, наприклад, для здобуття репутації, здійснення корпоративного шпигунства або в рамках

хакерської кампанії національної держави. Хакерів з білим капелюхом можна розглядати як «хороших хлопців», які намагаються запобігти успіху чорних хакерів шляхом активного злому. Вони використовують свої технічні навички для проникнення в системи для оцінки та перевірки рівня безпеки мережі, також відомого як етичний злом.

Хакери сірого капелюха. Сірі хакери сидять десь між хорошими і поганими хлопцями. На відміну від чорних хакерів, вони намагаються порушити стандарти та принципи, але без наміру завдати шкоди чи отримати фінансову вигоду.

Є кілька ключових кроків і найкращих практик, яких організації та користувачі можуть дотримуватися, щоб переконатися, що вони обмежують свої шанси бути зламаними: оновлення програмного забезпечення, використання унікальних паролів для різних облікових записів, шифрування HTTPS, уникнення натискання оголошень або дивних посилань, змінення імені користувача за зомовчуванням та паролів на вашому маршрутизаторі та смарт-пристроях.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Данило ЖИРОНКІН

Харківський національний університет внутрішніх справ

ТЕХНОЛОГІЯ ТА ПОЛІЦІЯ В НІДЕРЛАНДАХ

З 2013 року в Нідерландах є одна національна поліція з 10 регіональними підрозділами та одним центральним підрозділом. З того часу було отримано більше розуміння технологічних розробок в поліцейській організації, а інноваційні процеси були ініційовані більш централізовано. У 2016 році в результаті інвентаризації було виявлено 130 технологічних проєктів, які виконувала Національна поліція Нідерландів (Ernst and Кор, 2018). Лише невелика частина проєктів дійшла до інноваційної стадії, в якій технологія була впроваджена в оперативну поліцейську практику. Поліцейські організації також повинні підготуватися до майбутніх розробок та впровадження технологій, щоб зберегти легітимність у цьому швидко мінливому середовищі. Поліція повинна мати уявлення про технологію, яку вона використовує та розвиває, а також уявлення про її вплив на розвиток суспільства, наприклад, використання телекамер. Які фактори сприяють або гальмують технологічні інноваційні процеси від початкового початку до впровадження в Національній поліції Нідерландів?

Сьогодні технології швидко розвиваються і підсилюють одна одну. Нові технології, такі як штучний інтелект, додатки для великих даних, Інтернет речей, мобільний Інтернет, робототехніка, автономні транспортні засоби, хмарні технології, зберігання енергії та 3D-друк, мають значний вплив на національну та міжнародну безпеку, створюючи нові чи різні форми та цілі. злочинності. Щоб впоратися з цими новими проблемами безпеки та новими формами злочинності, поліції доведеться рухатися вперед і відповідно адаптувати свою організацію та методи роботи. Технологія також надає нові перспективні інструменти для поліцейських.

Нові та інноваційні технології часто вже розроблені та готові до використання поліцейською організацією, але, як показано, змусити поліцію фактично почати використовувати цю технологію виявляється складним і залежить від багатьох соціальних та організаційних факторів, які мають вирішальне значення. Фактичне використання технологій у повсякденній рутині поліцейської практики залежить від гнучкої та індивідуальної підтримки з боку служб фасилітації, мотивації та наполегливості керівників проєктів та керівників поліції, чіткої організаційної структури та управління та відповідного своєчасного та відповідного прийняття рішень щодо розробка проєкту. Загалом, поліцейській організації потрібна чітка інноваційна стратегія та бачення технологій.

Мовний радник І. О. Гоголь

УДК 351.74:001.895](100)(06)

Валерія ЖУРБА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ КИТАЮ

Поліція Китаю почала використовувати сонячні окуляри, обладнані спеціальною технологією розпізнання облич для виявлення підозрюваних.

Окуляри підключені до внутрішньої бази даних, а це означає, що офіцери можуть швидко сканувати натовп під час розшуку втікачів.

Технології розпізнавання осіб необхідні правоохоронним органам у пошуку злочинців, для забезпечення безпеки у місцях масового скупчення людей, а також для аналізу великих даних, це не є зазіхання на недоторканність приватного життя, оскільки зйомка ведеться у громадських місцях, розповіли компанії-розробники цих компаній.

«Камера здатна за раз охоплювати 200 осіб. У системі є база даних осіб, які перебувають у розшуку. Система здатна порівняти фото та подати сигнал при збігу», - розповів представник компанії.

За даними китайських державних ЗМІ, сонцезахисні окуляри вже допомогли поліції схопити сім підозрюваних.

Технологія дозволяє працівникам поліції сфотографувати підозрілу особу, а потім порівняти її з фотографіями, що зберігаються у внутрішніх даних. Якщо є відповідність, то інформація про ім'я особи та адресу буде надіслана офіцеру.

Також окуляри підтримують функції розпізнавання голосу та управління жестами. З усіма цими функціями GLXSS важить всього 55 грамів. В окуляри вбудовано 0,25-дюймовий видошукач з роздільною здатністю VGA.

Всі поліцейські на станції тепер використовують розумні окуляри для швидкої перевірки особи. На сьогодні поліції вдалося упіймати 7 втікачів і 26 власників підроблених документів на цій станції.

Китай є світовим лідером у технології розпізнавання облич та регулярно нагадує своїм громадянам, що завдяки такому обладнанню практично не можливо сховатись.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Єлизавета ЗАГОРЕЦЬКА

Віолетта КІРІЄНКО

Харківський національний університет внутрішніх справ

ЕКОЛОГІЧНА ЗЛОЧИННІСТЬ В УКРАЇНІ ТА ЗАРУБІЖНИХ КРАЇНАХ

У світі налічується близько 200 країн. Вони мають різний рівень економічного розвитку, різний стан добробуту, різні підходи до вирішення екологічних проблем. При цьому вони поділяють відповідальність за збереження та відновлення сприятливого стану навколишнього середовища на благо сьогодення та майбутніх поколінь. Коротко розглянемо досвід екологічного права в економічно розвинених країнах.

Заслуговує на увагу підхід іспанського кримінального права до проблеми збереження флори і фауни. ст. 334 Кримінального кодексу Іспанії передбачає відповідальність, якщо особа знищує види, яким загрожує зникнення в результаті полювання або рибальства, а також

здійснює діяльність, яка порушує або перешкоджає їх розмноженню або міграції, порушуючи закони або загальні положення про охорону видів лісових тварин. Ця норма забороняє торгівлю або транспортування цих видів або їх останків. Такі дії караються позбавленням волі на строк від шести місяців до двох років або штрафом від восьми до двадцяти восьми місяців.

18 листопада 2000 року було прийнято Екологічний кодекс Франції. Закон займає перше місце в ієрархії національного законодавства після Конституції. Екологічний кодекс Франції складається із Загальної та Особливої частин (975 статей). Загальна частина включає принцип, цілі та екологічну відповідальність. Особлива частина регламентує охорону природи, води та повітря. Відповідно до Кримінального кодексу Франції 1992 р. кримінальну відповідальність за екологічні правопорушення несуть усі юридичні особи, крім державних, адміністративно-територіальних утворень та їх об'єднань. Основними видами покарання для них є штрафи та обмеження їх діяльності. Максимальний розмір штрафу, накладеного на юридичну особу, дорівнює дев'ятикратному розміру максимального штрафу, накладеного на фізичну особу.

Згідно із законодавством США, за кримінальне порушення окремих положень Закону про управління водою, повітрям та відходами може бути накладено кримінальний штраф у розмірі до 25 000 доларів США за день порушення, або позбавлення волі на строк до одного року, або обидва. У разі повторного порушення – штраф до 50 000 доларів США за день порушення або позбавлення волі на строк до 2 років. Кримінальна відповідальність за екологічні правопорушення в США накладається за кримінальне порушення закону.

Однією з найбільш екологічно чистих країн світу є Об'єднані Арабські Емірати. Новий Кодекс ОАЕ, який повністю присвячений екологічним правопорушенням, включає 105 статей і, як повідомляється, включає штрафи за забруднення води, забруднення ґрунту, пошкодження природних заповідників, зелених насаджень тощо. За особливо тяжкий злочин проти природи – зараження ядерними відходами – Кодекс може розглянути можливість засудження.

Тому порівняльний аналіз зарубіжного законодавства про охорону навколишнього середовища є дуже цікавим для вивчення, а позитивний досвід може бути використаний для вдосконалення українського законодавства. Деякі законодавчі норми становлять особливий науковий інтерес і заслуговують на доопрацювання, наприклад, запровадження покарань для осіб, які повідомляють про випадки браконьєрства, запровадження норм, що передбачають відповідальність юридичних осіб за екологічні злочини (наприклад, Франція, США), усиновлення

Екологічного кодексу. На основі аналізу чинного законодавства, українського та зарубіжного правового досвіду у сфері забезпечення реалізації права на сприятливі екологічні умови необхідно закріпити ці закони в українському законодавстві як правову гарантію, а також соціальну, господарські та інші закони громадян.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Олена ЗАГОРУЙКО

Харківський національний університет внутрішніх справ

РОБОТ-ПОЛІЦЕЙСЬКИЙ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ У КАЛІФОРНІЇ

Правоохоронна діяльність завжди була і залишається основоположною для будь-якого цивілізованого демократичного суспільства. Усі етапи розвитку соціуму неминуче призводять до модернізації правоохоронної сфери, а розвиток технологій вимагає від органів внутрішніх справ поновому підходити до виконання повсякденних обов'язків, регулярно оновлювати методологію створення умов для безпечного існування людей.

Американський інженер Рубен Брюер із некомерційного дослідницького інституту SRI International (Каліфорнія, США) створив робота, який допомагатиме дорожній поліції. Прототип пройшов перші тести, він здатний перевіряти документи у водія та виписувати штрафні квитанції. Щороку співробітники поліції США перевіряють кілька мільйонів водіїв та автомобілів. Понад 190 тисяч разів під час огляду було застосовано фізичну силу. Понад 4 тисячі співробітників зазнавали нападів, деякі загинули. За такого розвитку подій робот стає необхідним рішенням. Робот складається з «тіла» зі сканером для документів, принтером та «голови» у залізній «фуражці» з камерою та екраном для спілкування з водієм. Після зупинки автомобіля, що перевіряється, робот «їде» до вікна водія і оглядає його за допомогою відеокамери. Перевірка документів здійснюється за допомогою сканера, а вбудований принтер може роздрукувати штрафну квитанцію. У разі потреби оператор-патрульний може переговорити з підозрілим водієм через робота. Щоб потенційний порушник не втік під час перевірки під дном автомобіля робот встановлює планку з шипами.

Як висновок можна зазначити, що інноваційні технології – це запорука розвитку правоохоронного відомства, інструмент, який стає реальною зброєю у боротьбі зі злочинністю. Завдяки розробленим

науковцями і фахівцями правоохоронної сфери пропозиціям та рекомендаціям, а також спільним зусиллям іноземних партнерів, депутатського корпусу, урядовців, керівників зацікавлених відомств може бути забезпечено реальне впровадження в практику всіх інновацій, які сприятимуть зниженню рівня злочинності. Країна, яка буде володіти потужними інформаційними ресурсами, ефективною системою їх реалізації, буде знати динаміку й перспективи їх розвитку, опиниться на гребні науково-технічного прогресу і зможе його ефективно використовувати.

Консультант з мови **Н. В. Краснова**

УДК 351.74:001.895](100)(06)

Наталія ЗАДОРЖНА

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ПОЛІЦІЇ НА ПРИКЛАДІ УКРАЇНИ І США

Боротьба зі злочинністю ведеться в Україні широким фронтом різними державними органами, громадськими організаціями. Важлива роль у цій діяльності належить правоохоронним органам, для яких боротьба зі злочинністю є основною функцією.

Значною мірою сьогодні ефективність діяльності правоохоронних органів залежить від технічного оснащення. В практичну діяльність органів Національної поліції України сьогодні широко впроваджується обчислювальна техніка, створюються локальні мережі, автоматизовані робочі місця, які обладнані сучасними потужними персональними комп'ютерами та базами даних. Все це дозволяє звільнити практичних працівників від виконання одноманітних операцій, допомагає знаходити оптимальні рішення при розв'язанні різноманітних питань, дає можливість глибше вивчати процеси, деталізувати їх, забезпечує можливість одночасного розгляду значної кількості фактів у взаємозв'язку та залежності при одночасній обробці різноманітної інформації.

Але, інноваційні технології в Україні ще не досягли високого рівня. Поліція, звертаючись до поліцейських заходів, зокрема, до зупинення транспортних засобів, може зустріти неадекватну, а інколи й небезпечну реакцію з боку водія. У США, де носіння зброї є конституційним правом особи, такі випадки непоодинокі.

Тому був винайдений trafficstoprobot — аналог, який може діяти замість реальної людини та знизити ризики від використання

вогнепальної зброї. Функціонал робота включає сканування водійських посвідчень, видачу штрафних квитанцій, затримання водіїв за допомогою «spikearm».

Таким чином, інформаційні технології є невід'ємною частиною діяльності поліції в різних країнах для боротьби зі злочинністю і досвід різних країн необхідно вивчати та впроваджувати.

Консультант з мови **Н. В. Краснова**

УДК 351.74:001.895](100)(06)

Катерина КАЛУГІНА

Харківський національний університет внутрішніх справ

КОМПОНЕНТИ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

Світова цифрова трансформація поставила перед безпекою та безпекою цифрових даних все більше проблем. Занепокоєння щодо володіння персональними даними та їх використання виникають у всьому світі. Відбулося різке збільшення частоти, швидкості, складності, серйозності та впливу кібератак на компанії та організації в усьому світі. Які найкращі методи захисту особистої інформації та цілісності цифрових систем, звільняючи місце для інновацій, які обіцяють нові технології?

П'ять компонентів системи управління ризиками кібербезпеки.

За словами Стівена Р. Чабінського, партнера White & Case у Вашингтоні, ефективна система управління ризиками кібербезпеки має п'ять основних компонентів. Вони включають:

Розгляд конкретних технологічних ризиків, з якими стикається компанія, і встановлення пріоритетів.

Здійснення належного захисту у вигляді технічного, адміністративного та фізичного контролю.

Здатність виявляти та правильно оцінювати інциденти безпеки.

Здатність швидко реагувати на порушення та об'єднувати всі підрозділи компанії, щоб запобігти загостренню порушення, одночасно ефективно спілкуючись і дотримуючись будь-яких юридичних та договірних зобов'язань.

Можливість відновитися після кібератаки, повернутися до справи та переконатися, що проблема не повториться.

Керівник відділу кібербезпеки повинен бути в змозі передбачити ймовірний вплив злому або хакерської атаки, яка робить конфіденційні дані або цілі мережі недоступними, а також важливо визначити наслідки

для бренду, його операцій та фінансів. Головне, каже Чабінський, — мати адекватні, відповідні для бізнесу заходи напередодні інциденту та навчений персонал, як їх застосовувати. Сканування вразливостей, щорічні оцінки ризиків і сторонні тести на проникнення надзвичайно корисні, а також письмові плани, які можуть бути корисними на будь-який випадок. Є також очевидні переваги використання обмежень на основі ролей для обмеження доступу співробітників до конфіденційних даних або можливості додавати або змінювати програмне забезпечення, використання багатфакторної автентифікації для входу в конфіденційні або віддалені системи, а також використання шифрування збережених або переданих даних. Іншим ключовим контролем є ефективна стратегія резервного копіювання даних, які втрачені або зловмисно знищені.

Що стосується можливостей виявлення, Чабінський застерігає, що старі продукти безпеки більше не є гарантією від кібератак, оскільки хакери постійно змінюють свої методи, і додає, що настільні вправи на основі сценаріїв довели ефективний досвід навчання для компаній, стурбованих порушенням перевірити їх готовність ефективно реагувати в усій організації.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Євгенія КАЛЮЖНА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Технології стали поширені в більшості сфер суспільства, і, намагаючись не відставати від останніх досягнень, державні установи змушені вводити інновації з зростаючими темпами. Технології змінюють роботу поліції в 21 столітті, запроваджуючи нові інструменти для боротьби зі злочинністю. Застосування таких технологій, однак, не є простим і залежить від багатьох людей. І, звичайно, остаточне рішення щодо використання тих чи інших технологій приймається після експерименту «Як це буде працювати на практиці».

Тому зараз я познайомлю вас із деякими сучасними технологіями, які значно спростили роботу поліції та потенційно змогли змінити гру в протидії злочинності.

По-перше, боді- камери (камери для носіння на тілі). Вони широко використовуються правоохоронними органами в різних країнах, включаючи Україну. Їх в основному носять офіцери під час виконання службових обов'язків, які потребують відкритого та безпосереднього

контакту з громадянами. А також допомагає зібрати інформацію та в разі потреби пред'явити її слідству для подання як докази.

По-друге, відео-домофони. Вони були встановлені тисячами домовласників, щоб підвищити безпеку свого будинку та забезпечити їм спокій. І вони допомагають поліції автоматично надіслати запит до власників камер, щоб одержати відеозаписи, місця злочину, біля якого вони мешкають.

По-третє, біометричні дані. Сьогодні правоохоронці мають у своєму розпорядженні безліч біометричних інструментів. Ця широка категорія включає в себе програму для ідентифікації злочинців, автоматизовані системи ідентифікації відбитків пальців (AFIS), автоматизовані системи біометричної ідентифікації (ABIS) і розпізнавання обличчя.

На завершення, цифрові технології зараз відіграють важливу роль у поліцейській діяльності та управлінні безпекою, оскільки поліцейські програми, дрони та камери для носіння на тілі та інші технології не припиняють розвиватися та допомагають швидше розкривати злочини.

Науковий керівник Н. Л. Горбач

УДК 351.74:001.895](100)(06)

Марія КАНАВЧЕНКО

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ

Науково-технічний прогрес, без перебільшення, можна вважати способом життя сучасної людини. В Україні значна увага приділяється розвитку інновацій, швидким темпам науково-технічного розвитку науки та техніки. Проте в останні роки через недостатнє фінансування, зокрема державне, та через відсутність зв'язку між вченими та споживачами інноваційної продукції переважна більшість показників, що характеризують інноваційну діяльність в Україні, поступово погіршуються.

Сьогодні співробітникам правоохоронних органів потрібна висока швидкість отримання необхідної інформації, її накопичення та оцінки. Спільно з вченими кафедри кримінології Національного юридичного університету імені Ярослава Мудрого для потреб правоохоронних органів було розроблено низку інноваційних продуктів, захищених низкою охоронних документів. Зокрема, отримано 3 патенти на винаходи та 8 свідоцтв про реєстрацію авторських прав на твори наукового характеру.

Є наступні інноваційні результати:

1. Розроблена Інститутом дослідження злочинності «Метод ідентифікації особи за параметрами мовлення» — це математична модель швидкого вейвлет - перетворення звукових сигналів за допомогою квадратурних дзеркальних фільтрів. Основою цієї моделі є найбільш ефективні методи та алгоритми - зображення сигналів різної фізичної природи. В ході експериментальних досліджень було виявлено, що використання запропонованої моделі для вирішення ідентифікаційних експертних завдань дозволяє скоротити час на дослідження та отримати більш точні результати.

2. Створений спільними зусиллями співробітників Інституту вивчення злочинності та вчених відділу кримінології «Прилад для вимірювання швидкості балістичного об'єкта» компактний, точний, простий у використанні. Дуже важливо, щоб після експериментальних пострілів поверхня балістичного об'єкта залишалася цілою. Прилад рекомендовано Харківським науково-дослідним криміналістичним центром МВС України для використання під час судово-балістичних експертиз.

3. «Автоматизоване робоче місце слідчого «Інсайт», призначене для оптимізації роботи слідчих, суддів, адвокатів. Автоматизоване робоче місце слідчого «Інсайт» використовується в педагогічній та науковій діяльності у сфері криміналістики та криміналістики, для вдосконалення навички практиків правоохоронних органів України.

Співробітниками кафедри кримінології для потреб правоохоронних органів сформовано понад 30 спеціалізованих комплектів науково-технічних засобів, а саме:

- 1) Універсальний судово-медичний набір слідчого;
- 2) Криміналістичний набір для роботи зі слідами;
- 3) Криміналістичний набір для роботи з мікрооб'єктами;
- 4) Криміналістичні набори «Валіза пожежного» та «Валіза слідчого»;
- 5) Набір науково-технічних засобів працівника митниці;
- 6) Чемодан відбитків пальців;
- 7) Набір науково-технічних засобів для геологорозвідувальних робіт;
- 8) Універсальний криміналістичний комплект;
- 9) Технічний комплект криміналістичного комплекту слідчого;

Розроблено багато науково-технічних засобів, які покращили роботу поліції. Це допомогло їм полегшити роботу зі слідами, мікрооб'єктами у надзвичайних ситуаціях. Це допомагає поліцейським краще виконувати свою роботу. Тобто в Україні розвивається науково - технічний прогрес.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Аліса КАНЮК

Харківський національний університет внутрішніх справ

НОВІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Поліцейські організації на міжнародному рівні досліджують та експериментують з новими технологіями, щоб покращити свою роботу у відповідь на нові форми злочинності.

Нові технології, такі як штучний інтелект, додатки для великих даних, Інтернет речей, мобільний Інтернет, робототехніка, автономні транспортні засоби, хмарні технології, зберігання енергії та 3D-друк, мають значний вплив на національну та міжнародну безпеку, створюючи нові або різні форми та цілі. Злочинності

Поліція може покращити свою роботу за допомогою інноваційної технології.

Поліція може ідентифікувати людей за біометричними відбитками пальців. У них також є натільна камера, якою вони знімають порушення. І звичайно нові швидкопрацюючі автомобілі.

На завершення я скажу, що для того, щоб впоратися з цими новими проблемами безпеки та новими формами злочинності, поліція повинна рухатися вперед і відповідно адаптувати свою організацію та методи роботи.

Науковий керівник Н. Л. Горбач

УДК 351.74:001.895](100)(06)

Богдан КАЧУРІН

Харківський національний університет внутрішніх справ

МАЙБУТНЄ ПРАВООХОРОННИХ ТЕХНОЛОГІЙ

Хоча багато відділів поліції вже деякий час використовують технології, деякі використовують новіші. Деякі новітні технології все ще знаходяться на теоретичній стадії, а інші призначені для обмежених сценаріїв у кожному конкретному випадку.

Прогнозна аналітика. Більша частина роботи поліції включає реагування на злочини чи інші інциденти; проте технології можуть дозволити поліції бути активними. Подумайте про прогнозу аналітику як про образливий підхід до громадської безпеки. Ця технологія виводить карту злочинності та збір даних на новий рівень, передбачаючи загальні області, де ймовірно майбутні злочини. Як виявив один відділ, така

інформація корисна для призначення та розподілу персоналу. «В одному прикладі, наведеному Національним інститутом юстиції, поліція Річмонда, штат Вірджинія, використала дані, щоб передбачити, де в новорічну ніч буде найбільше обстрілів. «До цих місць було направлено більше офіцерів, що призвело до зменшення обстрілів на 47% і збільшення вилученої зброї на 246%», – повідомляє The Press-Enterprise.

Тривимірне зображення місця злочину (3D). Тривимірне зображення місця злочину швидко стає незамінним аспектом роботи поліції. «Від швидкого збору даних на місці події до збереження їх для подальшого аналізу та створення ефективних презентацій для випробувань – лазерний сканер виявляється важливим інструментом для слідчих», – повідомляє PoliceOne. За допомогою цієї криміналістичної технології сканери фіксують 3D-модель місця злочину або нещасного випадку, що дозволяє отримати більш точні деталі. Офіцери можуть використовувати цю інформацію пізніше, щоб відновити ракурси та розміщення доказів або моделей бризок крові. Зйомка місця злочину в 3D означає, що офіцерам потрібно лише підтримувати повну сцену на час сканування, яке набагато коротше, ніж зазвичай. 3D-зображення також можуть убезпечити офіцерів на місцях аварії, оскільки менше часу на дослідження місця події означає, що вони швидше ліквідують зіткнення.

Персональний, наскрізний радар. Використання радару, щоб бачити крізь будівлі, — це ще один спосіб запобігти злочинності до того, як вона станеться. Радари працюють як тонко налаштовані детектори руху, використовуючи радіохвилі, щоб звести до нуля рухи, такі незначні, як дихання людини, на відстані понад 50 футів. Вони можуть визначити, чи є хтось у будинку, де вони перебувають і чи рухаються», – пише Бред Хіт в USA Today. Хоча наскрізний радар не є абсолютно новим, такі доповнення, як носимі комп'ютери та доповнена реальність, дозволяють офіцерам «бачити» крізь стіни і, відповідно, оцінювати загрози, як ніколи раніше.

Загалом, технології в правоохоронних органах створили багато переваг, які допомагають різним відомствам розкривати злочини, ідентифікувати підозрюваних і відстежувати їх. Більш ефективні такі види технологій дозволяють ловити злочинців і чинити опір правильно.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Діана КИРИЧЕНКО

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ДРОНІВ У ШВЕЦІЇ

Відома на весь світ як одне з найпрогресивніших та найщасливіших місць на землі, Швеція — пята за величиною країна в Європі. З року в рік якість життя у Швеції оцінюється набагато вищою, ніж в інших країнах. Багато в чому це відбувається завдяки тому, що шведська поліція відіграє велику роль у зниженні рівня злочинності та підвищенні рівня громадської безпеки.

У 2015 році управління поліції Швеції стало центральним органом управління шведською поліцією. Це стало помітною зміною після того, як десятки років підрозділи контролювали муніципальну владу. Вже ставши однією з передових країн із застосування нових технологій для захисту громадськості, Швеція почала вивчати використання дронів.

У країні офіційно запустили програму з використання поліцейських дронів у 2018 році. Поліцейським з кожного відділу було надано можливість взяти участь у програмі підвищення кваліфікації та пройти навчання з метою застосування дронів при виконанні службових обов'язків.

Швеція є країною, мабуть, найбільшою програмою з використання дронів для забезпечення громадської безпеки в Європі. Зважаючи на успішну діяльність шведського управління поліції у проведенні операцій із збереження громадської безпеки із застосуванням БПЛА, цей прогрес здається цілком природним.

Наприклад, відправлення дронів для фото- та відеозйомки до місць злочинів чи подій допомогло відділу поліції зменшити ризик втрати речових доказів. Поліцейські дрони також допомагають пожежним службам в аварійно-рятувальних роботах та в авіарозвідці за таких подій, як пожежі, розливи нафти та стихійні лиха.

Більше того, Швеція використовує дрони для забезпечення безпеки та управління натовпом під час великих масових заходів, таких як футбольні матчі, передвиборчі мітинги та демонстрації. Завдяки новим технологіям стало легше шукати зниклих в горах або в морі.

Дрони часто здійснюють польоти у громадських місцях неблагополучних районів, де випадки наркоторгівлі та правопорушень, які скоюють злочинні угруповання, зросли у 2019 році. Завдяки цим дронам, які доповнили піший патруль та інші заходи безпеки, що вживаються поліцією, запобігання та виявлення злочинів стало

простіше. Офіцери поліції піклуються про приватне життя громадян, тому вони мають право використання зйомки з повітря з метою розслідування та кримінального переслідування. Аерознімки та відео, що надаються як речовий доказ у суді, часто стають вирішальним фактором у справах без свідків. При цьому забезпечуються більш безпечні умови роботи для правоохоронців та рятувальників.

Робота, пов'язана з громадською безпекою, часто вимагає негайного прийняття рішень, тому дозвіл можна отримати, коли поліція прямує на місце події. Після отримання дозволу на використання дронів пілот повинен провести перевірку та дотримуватися дій, описаних у посібнику користувача. Загін реагування також повинен обов'язково подати до управління докладний звіт з описом кожного польоту.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Світлана КОБИЛІНСЬКА

Харківський національний університет внутрішніх справ

П'ЯТЬ ІННОВАЦІЙНИХ ПОЛІЦЕЙСЬКИХ ТЕХНОЛОГІЙ В ІЗРАЇЛІ

Технології змінюють роботу поліції у 21 столітті — впроваджують нові інструменти боротьби зі злочинністю та нові категорії злочинності. Ізраїльська поліція йде в ногу з часом, активно застосовуючи інноваційні технології у своїй роботі. Очікується, що в Тель-Авіві відбудеться виставка до початку Другої міжнародної конференції з внутрішньої безпеки, під час якої ізраїльська поліція продемонструє нові розробки, які допоможуть правоохоронцям боротися зі злочинністю.

Поліція Ізраїлю представить ряд інноваційних технологій, серед яких:

- «Eyeballs» — це мініатюрні відеокамери розміром з тенісні м'ячі, які можуть обертатися й отримувати інформацію на 360 градусів. Деякі камери мають менші розміри, менші громіздкості та довговічніші, а також кращу інтеграцію з автомобільними системами, щоб забезпечити синхронізоване відео події з кількох точок зору. Інші досягнення включають вищу роздільну здатність, чіткіший звук, ширші поля зору та підвищену стійкість до умов навколишнього середовища, таких як екстремальний холод.

- Інноваційний симулятор стрільби, який дає поліцейським можливість значно покращити свої навички поведінки зі зброєю в різноманітних ситуаціях, створених комп'ютером.

- Безпілотний літальний апарат. Безпілотники все частіше використовуються поліцією для отримання точок огляду з повітря для роботи на місці злочину, пошуку та порятунку, реконструкції аварій, моніторингу натовпу тощо. Ізраїль представляє повітряну кулю, яка використовується для повітряного спостереження, має об'єм всього 3 м³ (замість попереднього 20 м³), який легко поміщається в багажник автомобіля і керується з землі за допомогою спеціального смартфона.

- Голосова технологія. Однією з останніх інновацій, які впроваджуються в поліцейські машини, є нова технологія голосових команд, яка дає змогу офіцерам керувати багатьма функціями свого автомобіля під час керування та виконання інших патрульних обов'язків. Можливості цих голосових систем відрізняються від автомобіля до транспортного засобу, але більшість з них може обробляти команди, щоб запустити номерний знак або ввімкнути сирену. Більш просунуті та найперспективніші можливості технології голосових команд у поліцейських автомобілях значно полегшать подачу звітів — офіцери можуть диктувати свої нотатки, які потім реєструються безпосередньо в системі їхнього агентства.

- Автоматичне розпізнавання номерних знаків (ALPR). Та сама технологія, яка дозволяє платникам збору автоматично сканувати та збирати реєстраційні номери та літери на вашому номерному знаку для стягнення плати, зараз використовується поліцією для різних цілей правоохоронних органів. Той факт, що кілька камер можуть знімати один і той же номерний знак, потенційно дає поліцейським можливість відстежувати рух транспортного засобу з часом, розкриваючи подробиці про місцеперебування оператора, що, безумовно, може допомогти у лові злочинців.

Це не все, що може здивувати Ізраїль, тому можна з упевненістю сказати, що поліцейські технології розвиваються і не стоять на місці.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Божена КОВАЛЕНКО

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Зараз, у 21 столітті, в епоху технологій. Поліція теж не стоїть на місці, а розвивається, впроваджуючи щось нове. Наприклад, автоматичні сповіщення, камери тіла та відеореєстратор. Вони допомагають поліції

добре виконувати свою роботу. Автоматичні сповіщення скорочують час реагування

Правоохоронці не можуть реагувати швидше, ніж система, яка забезпечує їх інформацією. Завдяки мережевим відео- та аудіорішенням поліцейські можуть отримувати повідомлення про інциденти майже відразу, що значно скорочує час реагування. Мережеві камери – з інтегрованою аналітикою, датчиками та сигналізацією – відстежують зони високого рівня злочинності або місця, де громадяни відчувають загрозу, і надсилають автоматичні сповіщення в міру розвитку ситуації. Виявлення інцидентів і пряме відео з місця події допоможуть вам зрозуміти справжню природу інцидентів і відповідно розставити пріоритети. Інтегруючи гучномовці та прожектори в мережу, ви навіть можете зупинити злочини та правопорушення прямо в момент їх вчинення. Натільні камери дозволяють збирати цінні докази. А це, в свою чергу, ефективно попереджатиме небажану поведінку та позитивно вплине на дії операторів камер та громадськості. Розумна мережа відеоспостереження не лише допомагає запобігти злочинам, але й сприяє підвищенню засудженості та притягненню злочинців до відповідальності. Операційний центр надає офіцерам всю необхідну інформацію ще до прибуття на місце події. Знаючи, чого очікувати та на що слід звернути увагу, поліція на місці буде безпечнішою; крім того, це різко підвищить шанси на подальшу успішну роботу експертів-криміналістів. Розумна аналітика (наприклад, розпізнавання номерних знаків і обличчя) також може зробити вирішальний внесок у розслідування злочинів і затримання підозрюваних. Записи відеоспостереження також можна використовувати в суді.

Новітні технології дозволяють поліції працювати швидше, краще та незалежно.

Мовний радник І. О. Гоголь

УДК 351.74:001.895](100)(06)

Єлизавета КОВАЛЕНКО

Харківський національний університет внутрішніх справ

РОЛЬ ТЕХНОЛОГІЙ В ІНДІЙСЬКОМУ КРИМІНАЛЬНОМУ РОЗСЛІДУВАННІ

Технологія революціонізувала світ, у якому ми живемо. З кожного випадку, коли ми відкриваємо очі вранці, технології починають відігравати свою роль. Фактично, після події «Чорний лебідь» майже все було оцифровано. Від освіти, покупок, доставки їжі, транспорту та

банківських операцій і навіть офісів перемістилися до дому через різкий і далекосяжний вплив технологій. Технології кардинально змінили всі аспекти життя. У такому світі технологій, що швидко розвиваються, нашої поліції в кримінальному розслідуванні важливо пристебнутися та використовувати технології, щоб не відставати від поточного стану речей. Поліція вже включила багато технологічних аспектів, але час від часу виникає потреба в модернізації.

У зв'язку з прогресом у світі та стрімким зростанням у сфері технологій, для поліції важливо адаптуватися до мінливого світу. Зі мінливим світом злочини також розвинулися та набули нової форми, як-от кібер-залякування, крадіжка грошей, крадіжка даних, програм-викуп, підробка веб-сайтів, злом Інтернету речей тощо. у співвідношенні до поліції, необхідно мати технологію, щоб заповнювати складнощі та приймати своєчасні рішення. Інформаційні та комунікаційні технології – це метод надання складних послуг шляхом поєднання інформаційних технологій та телекомунікацій. ІКТ використовуються для зберігання, отримання, аналізу даних. Сюди також входить мобільний телефон, відеоконференції тощо. Ці технології ефективно використовуються поліцією для правоохоронних органів і можуть постійно вдосконалюватися для ефективного управління.

Використання технологій може бути дуже корисним у справедливих судах. У сьогоднішній час пандемії коронавірусу, коли рекомендується соціальне дистанціювання, ходити до переповненого суду вкрай небезпечно. Однак через цю пандемію багато справ могли залишитися на розгляді, купи матеріалів справ нагромадилися. Але технології прийшли нам на допомогу. Судові розгляди навіть тривають у цій пандемії завдяки можливості відеоконференції.

У сучасну епоху ми не можемо уявити дня без відповідної технології. Впровадження нових технологій є гострою вимогою навіть у кримінальному розслідуванні міліції. Багато технологій вже використовуються, але потрібне постійне оновлення. Технологія була благом, але були випадки грубого зловживання цими технологіями. Для попередження подібних випадків необхідно сформулювати законодавство. Технології дорогі, і тому ми повинні зосередитися на дослідженнях і розробках у нашій власній країні.

Мовний радник І. О. Гоголь

УДК 351.74:001.895](100)(06)

Єлизавета КОВАЛЕНКО

Харківський національний університет внутрішніх справ

ВІРТУАЛЬНА РЕАЛЬНІСТЬ У ПРОФІЛАКТИЦІ ДТП

Запобігання дорожньо-транспортним пригодам є одним із завдань дорожньої поліції, діяльність якої спрямована на зниження кількості дорожньо-транспортних пригод та підвищення відповідальності учасників дорожнього руху. Попередження ДТП спрямоване на всіх, особливо на вразливих учасників дорожнього руху, таких як велосипедисти та пішоходи.

Поліція землі Північного Рейну-Вестфалії запускає пілотний проект із тестування окулярів віртуальної реальності. Це відкриває нові можливості для запобігання дорожньо-транспортним пригодам. «За допомогою окулярів віртуальної реальності ми піднімаємо на новий рівень роботу щодо запобігання ДТП з тяжкими та дуже тяжкими наслідками», — заявив міністр внутрішніх справ Герберт Ройл.

Що стосується попередження ДТП, то поліція землі Північний Рейн-Вестфалія намагається зробити небезпеку дорожнього руху «відчутною». Використання окулярів віртуальної реальності дає можливість віртуально зануритися в дорожню ситуацію.

У 3D-фільмі, створеному поліцією Північного Рейну-Вестфалії, показана ситуація з велосипедистом та водієм вантажівки. Спочатку представлено сприйняття руху велосипедистом, користувачем окулярів віртуальної реальності, коли він усвідомлює, що водій вантажівки «втрачає його з зору» у так званій «сліпій зоні». У другому кадрі перспектива змінюється, і події спостерігаються вже з точки зору професійного водія. Ситуація, показана у фільмі, має показати учасникам дорожнього руху, наскільки обережними потрібно бути за кермом і як враховувати такі моменти.

«Альтернативні види транспорту, такі як велосипеди або використання велосипедів з електроприводом, дуже популярні і будуть у центрі нашої уваги ще більше в майбутньому, якщо йдеться про запобігання дорожньо-транспортним пригодам. Тому добре і правильно розпочати наш проект окулярів віртуальної реальності із цієї теми», — підтвердив міністр Ройл. «У велосипедистів немає ні зони зминання, ні подушки безпеки. Ми можемо це продемонструвати дуже яскраво за допомогою наших нових технічних можливостей».

Безпека - базова потреба людини, заради якої поліція готова зробити все потрібне. Запобігання ДТП має свої переваги, і тут велике значення можуть мати сучасні технології та системи штучного інтелекту.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Дмитро КОВАЛЬ

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ЗРАЗКІВ ДНК ДЛЯ КРИМІНАЛЬНИХ РОЗСЛІДУВАНЬ

Федеральна поліція Австралії (ФПА) використовує нову технологію, яка відкриває новий світ криміналістичного тестування ДНК для кримінальних розслідувань. Нова технологія, відома як Масивно Паралельне Узгодження (МПУ), може передбачати візуальні риси злочинців за ДНК, яку вони залишають на місці скоєння злочину, дозволяючи слідчим передбачати стать, біогеографічне походження, колір очей і, навіть, колір волосся. Біографічний прогноз походження порівнює ДНК з довідковою бібліотекою трьох груп населення древніх людей, що може допомогти виключити осіб, які цікавлять вас. ФПА ретельно тестує та оцінює МПУ, щоб забезпечити його точність, перед будь-яким використанням у судово-медичних розслідуваннях. Ця перевірка з метою використання в криміналістичному аналізі є першою в Австралії для правоохоронних органів. МПУ працює, досліджуючи послідовність нуклеотидних основ ДНК, яка присутня у зразках, зібраних на місці злочину, що є основним кодом для всього живого, включаючи людство.

Сучасні технології профілювання ДНК для ідентифікації людини досліджують варіації довжини геному людини, але МПУ досліджує нуклеотидну послідовність цих областей, що робить МПУ більш інформативним, ніж традиційне профілювання ДНК. Справжня сила технології МПУ полягає в її здатності отримувати дані з ДНК, коли злочинець невідомий і немає відповідного профілю в базі даних ДНК правоохоронних органів. Платформа також застосовується у справах про зниклих безвісти та непізнаних людських останків.

ФПА також зараз співпрацює з науковими колами та Земельних наук Австралії для розробки можливостей МПУ аналізувати ДНК навколишнього середовища як криміналістичного інструменту для профілювання ґрунту, ґрунту та води та досліджень наркотиків.

Протягом наступного десятиліття можливості прогнозування будуть розширюватися і включати такі ознаки, як вік, індекс маси тіла та зріст. Будуть шукатися можливості для надання тонких прогнозів для таких показників обличчя, як відстань між очима, форма ока, носа та вух, повнота губ і структура щік.

ФПА також дбає про збереження довіри громадськості та впевненості у використанні нових біотехнологій, і впровадила процеси

для мінімізації впливу на конфіденційність та захист будь-якої генетичної інформації.

*Науковий керівник **Олександр Олішевський***

УДК 351.74:001.895](100)(06)

Олександра КОЗЛЯНСЬКА

Харківський національний університет внутрішніх справ

РОЗВИТОК ГАЛУЗІ КРИМІНАЛЬНОГО ПРАВА

За словами Сейр Девіс з Університету Південної Юти, кримінальне правосуддя – це сфера карери, що швидко розвивається. Кожній країні світу потрібні працівники в цій сфері, і ця потреба ніколи не згасне. Оскільки технології розвиваються у цивільному світі, технології у світі кримінального правосуддя також розвиваються. Тут ми обговоримо абсолютно нові технології, які майже використовуються лише у сфері кримінального судочинства. Однак ми не будемо говорити про те, як цивільні програми та технології, такі як соціальні медіа, використовуються в правоохоронних органах, але їх важливо знати, якщо ви розглядаєте та вивчаєте цю тему. Ми обговоримо лише хмарні онлайн-системи, нові можливості виявлення, досягнення в тестуванні ДНК, технології до злочину, покращений захист і штучний інтелект.

Хмарні онлайн-системи. Одним з найефективніших досягнень у системі кримінального правосуддя є розробка хмарних онлайн-систем, які миттєво обмінюються інформацією з іншими співробітниками, а також іншими містами та штатами. Старий спосіб записувати все та зберігати це у файлах стає все менш звичним.

Тестування ДНК. Розвиток тестування ДНК змінив спосіб діяльності галузі. Колись ДНК не було доступно для допомоги у злочинах, які залишили багато справ нерозкритими. Тепер, коли це звичайна справа, прогрес у тестуванні ДНК швидко йде.

Здібності виявлення. Одним із найважливіших кроків для того, щоб правоохоронні органи добре виконували свою роботу, є здатність швидше виявляти та розкривати злочини.

Покращений захист. Необхідність захисту правоохоронців викликає дедалі більше занепокоєння через розвиток цивільних технологій, у тому числі у сфері вогнепальної та іншої зброї. Одним з найбільш швидкозростаючих і використовуваних покращених засобів захисту є «розумний ремінь». Розумний ремінь має систему, яка попереджає диспетчера та інших офіцерів, якщо пістолет або інший інструмент витягується з пояса. Цей інструмент дозволить пришвидшити резервне

копіювання, дозволяючи офіцерам мати безпечніший обмін, а також захищатися від судових позовів та інших речей.

Штучний інтелект. У правоохоронних органах найпоширеніший штучний інтелект (ШІ) вбудовується в бази даних, які вони використовують. Ці ШІ порівнюють злочини, минулі судимості, місцеположення, номерні знаки та багато іншого, щоб допомогти правоохоронним органам виявити злочинців. Багато з цього штучного інтелекту стають все більш ефективними та корисними.

Система кримінального правосуддя змінюється і стає все більш адаптованою до сучасного світу. Завдяки таким досягненням, як хмарні онлайн-системи, нові можливості виявлення, прогрес у тестуванні ДНК, покращений захист і штучний інтелект, система кримінального правосуддя стала ефективнішою та ефективнішою, ніж будь-коли.

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Катерина КОРЖ

Харківський національний університет внутрішніх справ

ДОСЛІДЖЕННЯ ЮРИДИЧНИХ ТЕХНОЛОГІЙ ДЛЯ СИСТЕМИ КРИМІНАЛЬНОЇ ЮСТИЦІЇ

Правові технології для системи кримінального правосуддя включають системи GPS, роботів, передові камери. Також задіяні високопродуктивні комп'ютерні системи та Інтернет-технології. Усі ці технології покращують спостереження та розслідування, спрощуючи процедури аналізу. Комп'ютерні програми ввійшли майже в усі сфери правоохоронної діяльності. Вони пов'язані з різними роботами, починаючи від роботизованих камер і закінчуючи тестуванням ДНК. Кількість електроніки та нових технологій у кримінальному судочинстві стрімко зростає. І всі вони мають одну мету – зробити роботу ефективнішою. Але це палка з двома кінцями, адже цими технологіями користуються і злочинці. Вони зловживають технологіями для незаконного використання. Сьогодні стає все більше технічно підкованих злочинців. Ось чому експерти з кримінального судочинства мають зробити крок далі в цій «технологічній боротьбі». Попри всі ці передові технології, буває, що когось несправедливо звинувачують. Тут на допомогу приходить адвокат із кримінальних справ. Адвокат повинен енергійно виступати за захист прав обвинувачених.

Існують деякі унікальні форми правової технології для системи кримінального правосуддя. Вони включають різні системи позиціонування та виявлення, такі як: системи ГІС та GPS – ці системи вже багато років існують у поліції. Офіцери використовують їх для

різних цілей. При визначенні підозрілого місця, пошуку найефективніших маршрутів тощо. Пройшли ті часи, коли поліцейським доводилося брати участь у швидкісній, небезпечній погоні. GPS допомагає їм відстежувати злочинців сьогодні набагато легше. Аналогічно, системи ГІС відстежують поліцейські машини. Це допомагає відділам визначити своє місцезнаходження в будь-який момент; Системи виявлення пострілів (GDS). Поліція часто встановлює системи електронних датчиків у зонах підвищеної злочинності. Це допомагає їм визначити, звідки лунає постріл. Таким чином офіцери мають кращий час реагування; Роботизовані камери, роботи та дрони. Роботи можуть замінити офіцерів у багатьох небезпечних ситуаціях. Таким чином, вони можуть перевірити небезпечні зони, розсіяти бомби тощо. Крім наземних роботів, існують і літаючі дрони. Ці пристрої забезпечують вид з висоти пташиного польоту, що корисно для багатьох місць злочинів. Вони особливо корисні у важкодоступних місцях; Автоматичні системи розпізнавання номерних знаків. Багато поліцейських автомобілів оснащені камерами, які можуть легко знімати номерні знаки. Це дозволяє офіцерам одразу побачити, викрадено автомобіль чи ні. І список юридичних технологій для системи кримінального правосуддя можна продовжувати. Є також камери, що носяться на тілі, наскрізні радары, програмне забезпечення для прогнозової аналітики тощо. Хоча деякі пристрої ще не повністю перевірені, інші пристрої є досить суперечливими.

Правоохоронні органи по всьому світу визнають цінність цих інструментів. Все більше відділів використовують нові технології для повсякденної діяльності. Проте багатьом ще потрібно навчитися ефективніше використовувати програмне забезпечення та комп'ютери. Це забезпечить їм успіх у майбутній кар'єрі.

Мовний радник І. О. Гоголь

УДК 351.74:001.895](100)(06)

Олена КОСТЕНКО

*Харківський національний педагогічний
університет імені Г. С. Сковороди*

ТРУДОВА ОСВІТА ЯК ОСВІТНЯ ІННОВАЦІЯ, НАПРАВЛЕНА НА СТВОРЕННЯ БЕЗПЕЧНОГО СОЦІАЛЬНОГО СЕРЕДОВИЩА

Враховуючи сучасні виклики, з якими стикається наша держава, необхідно приділяти особливу увагу створенню безпечного соціального середовища. У цьому контексті освітній процес стає вирішальним, оскільки формує нових членів суспільства.

Одним із методів виховання гармонійної особистості є трудове виховання. Незважаючи на те, що цей метод історично відомий, на сьогоднішній день в Україні його можна вважати педагогічною інновацією, оскільки він давно не використовується на практиці.

Історія української педагогіки добре знає педагогічну спадщину Софії Русової, Костянтина Ушинського, Антона Макаренка та інших, які використовували елементи трудового навчання у своїй педагогічній практиці. У цій роботі автор пропонує розглянути зарубіжний історичний досвід трудового виховання, виходячи з уявлень просвітителів про всебічний розвиток особистості, рівноправність і верховенство права.

Серед зарубіжних апологетів трудового виховання можна назвати Дж. Локка, Г. Песталоцці, К. Базедова, М. Монтеня, І. Фіхте. Бачення праці кожного з них має свої характерні риси. Усі вони підкреслюють творчу функцію праці. Вона повинна бути спрямована на формування всебічно розвиненої особистості. Через освіту, ставши частиною соціального габітусу людини, праця допомагає впоратися з негативними моделями поведінки.

Як педагогічна інновація, трудове виховання може передбачати активне включення елементів праці до навчально-виховного процесу, починаючи з самого раннього віку. При цьому необхідно неухильно дотримуватися принципу відповідності рівню складності, добровільності, розуміння значущості виконуваних завдань. Важливо підтримувати інтерес учнів. Враховуючи всі умови, метод трудового виховання міг би сприяти вихованню всебічно розвиненої особистості, яка буде привчена до праці. Це, у свою чергу, сприятиме створенню безпечного соціального середовища.

*Науковий керівник **Тетяна Чудовська***

УДК 351.74:001.895](100)(06)

Яна КРАВЧЕНКО

Харківський національний університет внутрішніх справ

КОМП'ЮТЕРНЕ ШАХРАЙСТВО ТА КІБЕРЗЛОЧИННІСТЬ У ПІВДЕННІЙ ФЛОРИДІ

Останнім часом правоохоронні органи Південної Флориди зосереджували увагу на вилученні та утриманні персональних комп'ютерів тих, хто перебуває під слідством за комп'ютерне шахрайство або кіберзлочинність. У боротьбі з комп'ютерним шахрайством та кіберзлочинністю поліція час від часу була виявлена, що проводить незаконні обшуки та вилучає персональні комп'ютери та інше пов'язане

майно. Тому вони пояснюють різницю між комп'ютерним шахрайством та кіберзлочинністю.

Комп'ютерні злочини – це злочинні дії, які вчиняються за допомогою комп'ютера.

Кіберзлочинність та Інтернет-злочинність зазвичай передбачає використання комп'ютера та Інтернету чи кіберпростору.

Комп'ютерні злочини, кіберзлочини та злочини в Інтернеті можуть бути «докомп'ютерними» злочинами, які існували до появи комп'ютера, такими як: розтрата, шахрайство, фінансові шахрайства, крадіжка особистих даних, переслідування тощо.

Вони також можуть включати злочини «сучасні технології», які почалися з впровадженням персональних комп'ютерів, мереж, кіберпростору та Інтернету: хакерство, фішинг (смішинг: SMS-повідомлення та фішинг; вішинг: голос і фішинг), фармінг, спам, програмне піратство, інформаційна війна, віруси, хробаки, атаки відмови в обслуговуванні, троянські коні, боти, зловмисне програмне забезпечення (зловмисний код), електронне шахрайство, кібер-переслідування, кібер-залякування, онлайн-хижаки, торгівля наркотиками тощо.

Комп'ютерні злочини, кіберзлочини та злочини в Інтернеті включають різні категорії злочинної діяльності. Міністерство юстиції США класифікує кіберзлочинність на 3 основні категорії:

1. Злочин незаконне отримання комп'ютерного обладнання та програмного забезпечення;

2. Злочини, спрямовані безпосередньо на Інтернет (чати, електронні листи, дошки оголошень і групи), комп'ютерні мережі, «хмару» або мобільні телефони (наприклад: злом комп'ютерів, віруси, хробаки; будь-яке небажане вторгнення в електронний пристрій) і

3. Злочини, скоєні за допомогою Інтернету, комп'ютерних мереж, хмари чи мобільних телефонів (наприклад: шахрайство та крадіжка особистих даних, фішинг, фармінг, електронні шахрайства, розкрадання, піратство програмного забезпечення, піратство музики, піратство фільмів, кібертероризм; дитина; дитина; порнографія, міжнародний шпигунство, фінансові крадіжки тощо).

У будь-якому випадку, запобігання, виявлення та пом'якшення наслідків – це частина захисту вашої особистості та підтримки хорошої репутації на фінансовій арені. Повідомлення про крадіжку та шахрайство є першим кроком до пом'якшення чи мінімізації збитків.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Катерина КУЗНІЧЕНКО

Харківський національний університет внутрішніх справ

КАМЕРИ ВІДЕОСПОСТЕРЕЖЕННЯ ЯК СПОСІБ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ

У всьому світі CCTV камери відеоспостереження стали основним заходом запобігання злочинності. Ця технологія вже застосовується в багатьох громадських місцях, таких як вокзали, аеропорти, офісні будівлі та на вулиці. Раніше камери відеоспостереження використовувалися як засіб для повідомлення про злочини, підтримки поліціантів у процесі судового переслідування або як докази, що підтверджуються в суді. Розвиток комп'ютерного зору та машинного навчання надає можливості для розслідування відеоспостереження як механізму запобігання злочинам. Камери відеоспостереження, як правило, призначені для зменшення злочинності за допомогою кількох механізмів.

По-перше, щоб утримати правопорушників, які бояться бути впізнаними, вчинити злочин на камеру.

По-друге, надати правоохоронним органам можливість виявляти злочини, які відбуваються або мають статися, надати їм можливість втрутитися.

Якщо ці два механізми виходять з ладу, камери відеоспостереження можуть зафіксувати докази того, що стався злочин, хто був причетний і що сталося, що може бути використано для кримінального переслідування.

Перший механізм ґрунтується на тому, що правопорушники усвідомлюють, що відеоспостереження ефективне, інакше не буде сприйнятого ризику.

Другий ґрунтується на тому, що співробітники контролюють канали камери та можуть виявляти підозрілу активність.

Третій ґрунтується на тому, що камера може зафіксувати поточну подію, яка може вимагати відповідного панорамування та нахилу.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Олександра КУЛАК

Харківський національний університет внутрішніх справ

МОБІЛІЗАЦІЙНІ ПРИСТРОЇ ДЛЯ МАЙБУТНЬОЇ ПОЛІЦЕЙСЬКОЇ СТРАТЕГІЇ

Хороша поліційна стратегія та технологія є допоміжними засобами до основної діяльності поліції. Одне без іншого не буде корисним в наш час. У зв'язку зі зміною політики правоохоронних органів дуже важливо визнати швидкість, з якою розвиваються також і технології. За допомогою технологій основний аспект яких є те, як громадськість реагує на різні стратегії та засоби, які використовуються правоохоронними органами для контролю злочинної діяльності, визначає ефективність нового пристрою в нашому суспільстві та чи буде він працювати, чи ні.

Наприклад, у США є додаток, відомий як Національний вебсайт сексуальних злочинців Департаменту юстиції, який відображає зареєстрованих сексуальних злочинців у радіусі навколо вас, і це дуже корисний інструмент, щоб інформувати поліцію, а також широку громадськість про їх оточення. З іншого боку, не зважаючи на те, що в деяких штатах є реєстр сексуальних злочинців, поліція ще не оприлюднила його. Скритність поліції для захисту приватного життя сексуальних злочинців є невігідною стратегією для суспільства. Наведений вище приклад також показує, що поліція повинна адаптуватися до нових стратегій і політики, які можуть відповісти на виклики, пов'язані з зростаючим рівнем злочинності навколо нас.

Ще одним технологічним засобом є розподільний віртуальний і сенсорний патруль. Використання технологій та докладання зусиль для отримання суттєвих результатів замість того, щоб розслідувати складні справи без належного обладнання, не тільки заощадить час та енергію, але й знизить рівень злочинності навколо нас. Навіть якщо для запобігання злочинам будуть створені окремі відділи з належною робочою силою, можливість фізичного перебування на місці злочину під час вчинення його практично неможлива. Таким чином, такі технології, як Інтернет речей (концепція обчислювальної мережі фізичних предметів, оснащених вбудованими технологіями для взаємодії один з одним або із зовнішнім середовищем), розумні датчики, камери відеоспостереження, є потребою часу, щоб з меншими зусиллями людей і більшою кількістю технологій поліція все ще могла стежити за суспільством і надавати доступ до безпрецедентної обізнаності. Ці засоби можуть надавати вихідні дані, які будуть використані для детальних досліджень та аналізу, щоб зробити розслідування швидким та ефективним.

Технології повинні бути достатньо розумними, щоб допомогти співробітникам поліції на місці скоєння злочину. Такі технологічні пристрої як мініатюризована електроніка, комунікації 5G, смарт окуляри, дрони для спостереження тощо, дозволяють поліції знаходити різні докази, які можуть залишитися непоміченими людським очам. Такі речі, як журнали попередніх викликів, локацій, реєстр злочинів тощо, є деякими прикладами засобів, які використовуються для стратегії та виконання рейдів, місій тощо. До переваг нових технологій також відноситься цифрове резервне копіювання в польових умовах. Простішими словами, дрони та камери використовуються на місцях як резервний захист.

*Науковий керівник **Олександр Олішевський***

УДК 351.74:001.895](100)(06)

Вікторія КУЛИК

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ГЕЛІКОПТЕРІВ У ПОЛІЦЕЙСЬКІЙ СЛУЖБІ

Федеральна поліція володіє парком гелікоптерів, який не має собі рівних у Європі з точки зору сучасного обладнання, ефективності та розмірів. Гелікоптери використовуються для виконання таких завдань, як патрулювання кордону та перевезення особового складу та спецпідрозділів. У коло завдань гелікоптерної ескадрильї поліції входить пошук злочинців, розшук зниклих безвісти, охорона громадського порядку під час проведення масових заходів. Гелікоптерна ескадрилья поліції також забезпечує підтримку підрозділів поліції особливого призначення.

Основним гелікоптером флоту є EC155, 5-тонний гелікоптер, який використовується в різноманітних операціях. Кабіна гелікоптера розрахована на 13 пасажирів і двох пілотів і може перевозити обладнання вагою до 2 тон. Сучасна кабіна оснащена цифровою авіонікою та автопілотом.

Низький рівень вібрації гелікоптера створює ідеальні умови для встановлення спеціального поліцейського обладнання. Обладнання Федеральної поліції включає камери денного та нічного бачення, потужні прожектори та гучномовці, 90-метровий кабель лебідки та систему аерофотозйомки та відеозйомки. Дані та записи надсилаються безпосередньо до командних та ситуаційних центрів місцевого управління поліції та МВС.

На додаток до EC155 B1, до парку вертольотів також входять вертольоти EC135 T2i для роботи поліції, ліквідації наслідків стихійних

лих і рятувальних операцій, вертоліт AS332 L1 Super Puma для транспортування на далекі відстані, управління повітряним рухом, в якості VIP- транспорту та EC120 для тренувальних польотів.

Протягом кількох років поліцейські гелікоптери мають серйозних конкурентів. Це безпілотні літальні апарати. Вони простіші та менш дорогі, ідеально підходять для візуального спостереження за місцевістю та перетинами вулиць, але можливості дронів обмежуються тільки цією функцією. Поліція використовує традиційні засоби повітряного транспорту – вертольоти, гвинтокрили і надалі забезпечуватимуть безпеку мешканців великих міст та віддалених регіонів країни та гарантуватимуть високу оперативну готовність.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Олександр КУРІЛКІН

Харківський національний університет внутрішніх справ

ЗМІНА ПОЛІЦЕЙСЬКОЇ ЕКОСИСТЕМИ ЗАРАДІ БЕЗПЕЧНОГО МАЙБУТНЬОГО

Ми живемо у світі, де рівень злочинності зростає з кожним днем, де гуманність ставиться під сумнів після кожного злочину, де тяжкість злочину зростає до небес, де суворіша політика правоохоронних органів важливіша, ніж релігійні сварки, які ми спостерігаємо навколо нас. У такому світі нові методології, технології та ідеї є потребою сьогодення. Правоохоронні органи, почавши з впровадження нових ідей, технологій, тощо, були збентежені новими концепціями, введеними у світ злочинності. Сьогодення потребує зміни поліцейської екосистеми для безпечнішого майбутнього.

Правоохоронні органи були створені, для забезпечення того, щоб кожен громадянин дотримується правил і правових норм, а кінцевим результатом було зберегти суспільство в безпеці, а світ кращим місцем для життя. Нові технології означають не лише технологічний прогрес. Нові стратегії, плани, ідеї, методи, тощо становлять невід'ємну частину нових технологій, що розвиваються. Нові технології можуть бути запроваджені лише за умови, що для поліції стануть притаманними почуття безкорисливої суспільної діяльності, почуття відповідальності, жертвовності та морально стійкої чесності. У сучасному світі щоденні досягнення передових технологій зривають дах появою нових технологічних пристроїв та послуг. Не поступаючись етичним кодексом, правоохоронні органи повинні свідомо сприймати нове середовище, що

розвивається, з динамічним ентузіазмом і реалістичною стратегією дій, щоб надати суспільству новий позитивний напрямок розвитку.

Необхідно сформулювати нові стратегії, пам'ятаючи про вплив як про активної, так і реактивної дій поліції на громаду та злочинність. Наприклад, програми викупу зброї. Програма включає в себе розвиток громади, оскільки особа, яка повертає втрачену зброю назад до поліції, отримує грошову винагороду. По-перше, ця програма була запроваджена, щоб прибрати всю незаконну зброю з вулиць і водночас залучити громаду до того, щоб зробити своє оточення та громаду безпечним місцем. Відсутність фінансування на техніку, озброєння, технології тощо призводить до погіршення стандартів розслідування. Розслідування порушуються через відсутність організованої взаємодії між різними підрозділами. Сучасні технології використовуються не в повному об'ємі часто не лишень за відсутністю кваліфікованих працівників поліції, а в кінцевому підсумку погіршують і стандарти підготовки. Засоби масової інформації дуже голосно висловлюють своє розчарування з приводу надзвичайно неефективної відповідальності осіб, яких поліція, як правило, приймає на роботу. Тому дуже необхідно внести зміни в екосистему поліції, яка створить безпечніше середовище для всіх.

*Науковий керівник **Олександр Олішевський***

УДК 351.74:001.895](100)(06)

Максим КУЩ

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ НОВІТНІХ КРИМІНАЛІСТИЧНИХ ЗАСОБІВ ТА ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ

Значною мірою ефективність діяльності правоохоронних органів залежить від технічного оснащення та використання інноваційних технологій у професійній діяльності працівників поліції. Осмислення прийдешніх форм стають вихідними пунктами в організації завдань і технічних ідей. Особливо це стосується інноваційного вектору розвитку, який вимагає від правоохоронних органів нового підходу до виконання службових обов'язків спрямованих на захист прав і свобод людини від протиправних посягань.

Використання новітніх криміналістичних засобів та інноваційних технологій, безумовно, сприяє оптимізації діяльності органів поліції у процесі боротьби зі злочинністю. Створюються локальні мережі, автоматизовані робочі місця, що дозволяє звільнити практичних працівників від виконання одноманітних операцій, забезпечує

можливість одночасного розгляду значної кількості фактів у взаємозв'язку та залежності при одночасній обробці різноманітної інформації. Особливої уваги заслуговує зарубіжний досвід використання інноваційних технологій в професійній діяльності працівників поліції.

Використання інноваційних технологій у роботі поліції зарубіжних країн умовно можна розподілити на дві основні категорії:

упредметнені технології (апаратні засоби чи матеріали);

нематеріальні технології (комп'ютерне програмне забезпечення, інформаційно - пошукові системи).

Упредметнені технології: покращений захист поліцейського обладнання, модифіковане озброєння, мобільний контроль за масовими заворушеннями, проєкт 54 – «вільні руки» патрульного за кермом, ідентифікація злочинців та громадян за допомогою біометричних даних, мобільні центри обробки даних.

Нематеріальні технології становлять відображення злочинності на карті, так звані «гарячі точки», діджиталізацію обміну інформацією в державному та приватному секторах, використання системи «бурштинове оповіщення». Зазначена система реагування на надзвичайні ситуації дозволяє працівникам поліції поширювати інформацію про зникнення людини за допомогою електронних знаків проїжджої частини.

Сполучені Штати Америки, Велика Британія та Європейський Союз планують запровадити більш точну ідентифікацію своїх баз даних за допомогою мультибіометрії. Тому державний сектор зазначених країн зацікавлений в прискореному розвитку біометричних технологій. Зараз проводиться експериментально-практичний етап роботи щодо можливості ідентифікації суб'єкта в будь-якій базі даних за одним із біометричних показників або одночасно за трьома основними видами ідентифікації особистості:

папілярними візерунками пальців;

райдужною оболонкою ока;

за допомогою оцифрованих фотозображень обличчя.

В даний час значна кількість інноваційних компаній розробляють математичні алгоритми та відеокамери для тривимірного (3D) або комбінованого (2D + 3D) зображень розпізнавання людських облич. Система відеоспостереження сучасних міст є фундаментальним компонентом інтегрованої системи безпеки. Відеозображення є важливим джерелом об'єктивної інформації про ситуацію, що дозволяє приймати правильні рішення в ситуаціях, що перебувають постійно в динаміці постійно змінюються.

Підсумовуючи можна сказати, що інформаційні технології у сфері комунікації, обробки інформації, компіляції даних, що використовуються на службі правоохоронних органів зарубіжних країн незабаром стануть

основою ери нового цифрового розслідування кримінальних правопорушень. Правоохоронні органи постійно розширюють джерела отримання та обробки інформації, активно використовують інформаційні системи для пошуку, зберігання та видачі облікових даних нового покоління.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Кирило МАКАРЕНКО

Харківський національний університет внутрішніх справ

ДРОНИ І РОБОТИ У ФОРМІ: ЯК ТЕХНОЛОГІЇ ЗМІНИЛИ ПОЛІЦІЮ

Середньорічний темп зростання світових витрат правоохоронних органів на програмне забезпечення та обладнання становить 9,3%. У 2018 році фінансування оцінювалося в 11,6 млрд. доларів, у 2020 році вже було витрачено більше 13,6 млрд. доларів, а до 2023 року, за оцінками аналітичної компанії, бюджет збільшиться до 18,1 млрд. доларів.

У США інженер-механік з каліфорнійського дослідницького інституту SRI International розробив робота, який допоможе поліцейським уникати потенційних конфліктів з автомобілістами.

Робот може сканувати документи водія та виписувати штраф, а щоб той не поїхав, він розкладає під колеса автомобіля брус із шипами. При цьому поліцейський може не виходити з машини, щоб не наражати себе на ризик.

Поки що новинка проходить випробування.

Ще одна система асистентів незабаром з'явиться у поліції Великої Британії. З її допомогою правоохоронці планують передбачати скоєння тяжких злочинів насильницького характеру за допомогою технологій штучного інтелекту.

National Data Analysis Solution (NDAS) використовує комбінацію штучного інтелекту та статистики. Для пошуку майбутніх злочинців система оцінює понад 1,4 тис. характеристик. Алгоритми штучного інтелекту обчислюють людину за рівнем ризику та оцінюють ймовірність скоєння злочину із застосуванням зброї.

В Індії стартап Staqu також розробляє низку допоміжних технологій для правоохоронних органів, таких як ABHED (Artificial Intelligence Based Human Efface Detection) – програма для розпізнавання відбитків пальців, обличчя та голосу.

Ще одна розробка індійських вчених – "розумні" окуляри на основі штучного інтелекту, які допоможуть поліції виявляти потенційних

злочинців у режимі реального часу. Вони оснащені камерами, які фотографують людей та звіряють знімки з базою даних злочинців. Якщо збіг знайдено, інформація відображається на вбудованому проекторі.

Натільні Камери

Натільні камери – це мобільні пристрої для запису відео. Таке обладнання активно використовувалося під час заворушень 2014 року у Фергюсоні, штат Міссурі. Тоді під тиском громадськості.

Президент США інвестував 263 мільйони доларів на придбання камер, які підвищать прозорість взаємодії поліції з громадянами.

Локатори пострілів

Оптичні та акустичні датчики з відновленням геопозиції дозволяють відстежувати зйомку. Наприклад, технології ShotSpotter використовуються більш ніж у ста містах Північної Америки та Південної Африки.

Підводячи підсумок, можна сказати, що метою даної роботи є не заміна професіоналів штучним інтелектом, а створення для них сучасного інструменту, який підвищить продуктивність працівників та зменшить витрати на оплату праці при проведенні правових та антикорупційних експертиз.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Микола МАКОВЧИК

Харківський національний університет внутрішніх справ

НОВИЙ ЗАСІБ СПОСТЕРЕЖЕННЯ ПОЛІЦІЇ КИТАЮ

Новітні технології спостереження було розроблено в Китаї, щоб розпізнавати людей за тим, як вони рухаються, або за формою їх тіла. Крім того, велика кількість камер відеоспостереження, які використовують передову оптику та технології розпізнавання обличчя, уже використовують цей інструмент на вулицях двох найбільших міст – Пекін та Шанхай. Це викликає стурбованість у прихильників конфіденційності щодо того, наскільки далеко уряд готовий зайти, щоб стежити за своїми громадянами.

Компанія, яка розробила систему, стверджує, що вона може ідентифікувати людей на відстані до 50 метрів (165 футів), навіть коли особи повернуті спиною або їх обличчя закриті.

Кожен комплект окулярів із функцією розпізнавання обличчя оснащено оптикою для розпізнавання обличчя, здатною точно

визначити одного втікача навіть у найбільш людних місцях, як-от залізничний вокзал чи аеропорт.

Окуляри автоматизують процес ідентифікації перехожих за лічені секунди і без неперевіршеної точності. Коли користувач дивиться в чийсь бік, прикріплена камера робить точні вимірювання ширини та глибини обличчя, перш ніж порівнювати його з базою даних ідентифікованих осіб.

Поліціанти Чженчжоу були помічені в сонцезахисних окулярах, оснащених програмним забезпеченням для розпізнавання облич, що дозволяє їм ідентифікувати людей у натовпі. Китай є лідером в галузі розвитку штучного інтелекту (ШІ) для спостереження. Так, наприклад, система відеоспостереження вистежила репортера Бі-Бі-Сі у сфері технологій всього за сім хвилин під час демонстрації.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Каріна МАЛИНОВСЬКА

Харківський національний університет внутрішніх справ

ІНТЕРНЕТ США ТА ВЕЛИКОЇ БРИТАНІЇ ЯК ДОПОМОГА У БОРОТБІ ЗІ ЗЛОЧИННІСТЮ

Незважаючи на окреслені проблеми та потенційні вразливості, можна вказати на Інтернет речей в цілому як на новий варіант використання щодо запобігання та виявлення злочинів. Наприклад, коли поліція почала використовувати розподілені датчики виявлення вогнепальних пострілів під назвою ShotSpotter у Камдені, штат Нью-Джерсі, вони виявили, що 38 відсотків пострілів в одному районі взагалі не повідомлялися або не виявлялися. Це дозволило поліції зосередити більше ресурсів на цій сфері, ніж це було раніше. Бачення майбутнього розумного міста передбачають підключені пристрої, які керують транспортними потоками, громадське освітлення та інші системи. Якби ці системи були інтегровані з датчиками та камерами по всьому місту, вони могли б мати величезний потенціал для виявлення злочинів. Однією з ідей є інтеграція ShotSpotter з підключеними системами вуличного освітлення, щоб допомогти реагувати на інциденти з вогнепальною зброєю. Нещодавній коментар у американському журналі Police Chief Magazine намалював картину: «З інтегрованим технологічним підходом Safe Cities, після розрядження вогнепальної зброї, вуличні ліхтарі в цьому районі (за умови, що в цей час темніло) будуть негайно доведені до більшої яскравості. Обладнання відеоспостереження в

цьому районі буде активовано і повернуто в напрямку обстрілу, а зчитувачі номерних знаків будуть активовані, щоб фіксувати номерні знаки в цьому районі. Відео буде знято та передане до командно-диспетчерського пункту, а потім передано офіцерам, які відповідають».

Більш широко, потенційний потенціал полягає в тому, що за наявності достатньої кількості підключених пристроїв правоохоронці зможуть швидко дізнатися, у справах про серйозні злочини, де перебували потенційні підозрювані на момент злочину, з ким вони були та ким вони були. робити. Система поінформованості про домен, яка вже використовується Департаментом поліції Нью-Йорка, вже рухається в цьому напрямку.

Очевидно, що зараз з'являються випадки, коли докази, зібрані з пристроїв, підключених до Інтернету, виявляються вирішальними для проведення арештів. У Великобританії було розкрито один випадок багаторазової крадіжки зі зломом після того, як маршрутизатори BT Wi-Fi були досліджені в ряду з чотирьох будинків, кожен з яких був зламаний в середині дня. Маршрутизатори показали, що один і той самий мобільний телефон підключався до безкоштовної послуги BT-FON у кожному з будинків у день крадіжок. Поліція використала цю інформацію, щоб розшукати зловмисника.

Технологія блокчейн може означати для поліції та злочинності, Інтернет є двосічним мечем для правоохоронних органів. Однак наявність недоліків лише робить ще більш важливим те, що поліція використовує можливості Інтернету.

*Консультант з мови **В. В. Кочина***

УДК 351.74:001.895](100)(06)

Дмитро МАЛЯРЕНКО

Владислав ШУВАЛОВ

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В РОБОТІ ПОЛІЦІЇ

Технології змінюють роботу поліції в 21 столітті, впроваджуючи нові інструменти для боротьби зі злочинністю, але з розвитком технологій змінюються можливості вчинення злочинів. Наприклад поліцейські департаменти у різних країнах застосовують дрони для спостереження з неба, поліцейські використовують натільні камери для зняття своїх дій на плівку.

Програмне забезпечення з розпізнавання обличчя. Одна з найбільш суперечливих нових поліцейських технологій передбачає

використання програмного забезпечення для розпізнавання обличчя. Коли цей інструмент вперше потрапив у розпорядження правоохоронних органів, багато хто вважав, що його використання не є неетичним. На щастя, це не так, і розпізнавання обличчя виявляється ефективним інструментом розслідування.

Біометрія. Поліція вже більше століття використовує відбитки пальців для ідентифікації людей. Тепер, окрім розпізнавання обличчя і ДНК, правоохоронні органи та розвідувальні органи користуються постійно зростаючим набором біометричних (і поведінкових) характеристик. Таких як розпізнавання голосу, відбитки долонь, вени на зап'ястях, розпізнавання райдужної оболонки ока, аналіз ходи і навіть серцебиття.

Роботи. Зараз багато правоохоронних органів використовують роботів з камерами нового покоління для відео та аудіо спостереження потенціальних місць злочину.

Виявлення пострілу. Використовуючи картографію та електронні датчики, виявлення вогнепальних пострілів дозволяє офіцерам негайно та точно реагувати.

Збір даних та аналіз злочинності. Швидке відстеження та аналіз великої кількості даних важливі для того, щоб правоохоронні органи ефективно виконували свою роботу. За допомогою хмарних обчислень поліція може отримати доступ до точної статистики та інформаційних панелей у реальному часі.

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Денис МЕДЯНИК

Харківський національний університет внутрішніх справ

РОБОТОТЕХНІКА НА СЛУЖБІ В ПОЛІЦІЇ

За останні роки людство досягло великих успіхів у сфері техніки, яка фактично торкнулася всіх сфер людської діяльності. Найрозвиненіші країни світу все частіше починають використовувати автоматизовані системи в різних сферах, у тому числі у поліцейській діяльності.

Важко визначити, яка країна вперше використала робототехніку на патрульних дільницях, але на даний момент у поліцейській діяльності роботи використовуються в США, Об'єднаних Арабських Еміратах, Китаї, в Казахстані, Сінгапурі та інших країнах.

Так, у Каліфорнії вже можна знайти роботів, які можуть пересуватися з метою оцінки ситуації як спокійної або небезпечної. Такі роботи

працюють як помічники або поліцейські у кількох торгових центрах та офісах великих технологічних компаній. Інший пристрій під назвою REEM's work, запущений в Об'єднаних Арабських Еміратах, може захистити людей від жорстокості, оскільки може негайно передати в центр управління те, що відбувається. Люди можуть використовувати його, щоб повідомити про злочин, сплатити штрафи та отримати інформацію, торкаючись сенсорного екрана.

У наш час інноваційні технології дуже важливі, це те, що значно полегшує наше життя (смартфони, які можуть з нами розмовляти, автовідповіді, розумні пристрої та всі інші чудеса, викликані розвитком технологій (D'après «Les nouvelles de France» <https://www.france24.com/fr>). Так, в Тунісі вирішили, що робот поліцейський патрулюватиме вулицями для того, щоб мешканці міста не порушували правил ізоляції.

(D'après «le Portail du ministère de l'intérieur» <https://www.interieur.gov.tn>

Робокоп рухається на колесах, контролюється дистанційно, оснащений інфрачервоними та тепловими камерами, а також звуковою та світловою сигналізацією. У саундтреках та відео, розміщених на сайті міністерства внутрішніх справ Тунісу, видно як робот звертається до осіб, які підозрюються у порушенні карантинних вимог: «Що ти робиш? Покажи свій паспорт. Ти не знаєш, що маєш залишитися вдома?»

Робот передає сигнал та зображення зловмисника, ідентифікуючи його у найближчому відділенні поліції.

Аніс Сахбані, туніський дизайнер роботи, сказав, що робот був запущений в перший раз у 2015 році для того, щоб патрулювати вулиці.

Він каже, що автоматизована машина працює в автономному режимі завдяки штучному інтелекту.

Різні модифікації робота коштують від 100 до 140 тисяч доларів та використовуються головним чином іноземними підприємствами з метою забезпечення безпеки.

В Японії такі роботи можуть бути задіяні майже скрізь, від продуктових крамниць до клінічних лабораторій. Але питання ще залишається відкритим щодо використання роботів, запрограмованих на на забезпечення громадського порядку.

Сьогодні мова ще не йде про загальне використання роботів та штучного інтелекту в поліції, міністерство внутрішніх справ України поки ще не готове до заміни поліцейських на вулицях роботами. Але подібна демонстрація результатів наукового та технічного прогресу є вдалою та дуже перспективною. Це лише питання часу. На підставі вивчення світового досвіду можна зробити висновок, що використання роботів в діяльності поліцейських допоможе зробити таку діяльність безпечною та ефективною. На мою думку, використання робототехніки

у службі дільничних офіцерів поліції могло б стати перспективним напрямком правоохоронної діяльності.

Науковий керівник І. Л. Іванова

УДК 351.74:001.895](100)(06)

Ліна МИЦИК

Харківський національний університет внутрішніх справ

ЯК ПОЛІЦІЯ ТОКІО ВИКОРИСТОВУЄ ДРОНИ

У 2015 році безпілотною «Фантом-2» з невеликою кількістю радіоактивного піску здійснив посадку на дах канцелярії прем'єр-міністра Японії. Цей акт був скоріше протестом проти ядерної енергетичної політики країни, ніж серйозною загрозою, але японці, очевидно, розцінили це як тривожний сигнал. Ніхто не постраждав, і правопорушника згодом затримали у зв'язку з інцидентом.

Для того, щоб у майбутньому боротися з такими загрозами з повітря, Департамент поліції м.Токіо представив безпілотною перехоплювач, оснащений сіткою, який має бути використаний, щоб ловити шахрайські квадрокоптери.

У Департаменті поліції м.Токіо було створено загін безпілотною, призначений для виявлення та, якщо необхідно, захоплення підозрілих дронів, якими керують громадяни. Підрозділ поліції патрулює територію біля важливих об'єктів, таких як резиденція прем'єр-міністра. Якщо буде виявлений підозрілий дрон, оператора попередять через гучномовці, які розташовані на землі. Але якщо оператор не відреагує, поліція запустить дрони, оснащені сітками, щоб зловити пристрій.

Квадрокоптери поліції Токіо в комплекті з сітками можуть зловити небажаний пристрій, що знаходиться в повітрі. В Японії заборонено керувати безпілотною над певними районами, такими як аеропорти та електростанції, над дорогами або на висоті понад 150 метрів. Деякі міста, такі як Токіо та Осака, також заборонили використання дронів у парках.

Положення про дрони набуло чинності в Японії після внесення поправок до Закону про Сили Самооборони країни. Новий японський дрон із сіткою, який знищує дрони, безумовно, є цікавим способом охорони тих районів, де вони заборонені.

У кількох країнах посилюють правила використання дронів. У США, наприклад, влада закликала створити реєстр дронів, у якому будуть перелічені власники пристроїв по всій країні.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Максим МІНЯЙЛО

Харківський національний університет внутрішніх справ

ТЕХНОЛОГІЧНІ ІННОВАЦІЇ НА СЛУЖБІ ПОЛІЦІЇ ТА ПОПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ

Розроблено нові технологічні інновації для запобігання злочинності та покращення роботи поліції. Інновації в технологіях кримінального судочинства можна розділити на дві великі категорії: жорсткі технології (апаратні засоби або матеріали) і м'які технології (комп'ютерне програмне забезпечення, інформаційні системи). Жорсткі технологічні інновації включають нові матеріали, пристрої та обладнання, які можна використовувати як для вчинення злочинів, так і для запобігання злочинам і боротьби з ними. Існують апаратні технології, призначені для запобігання злочинам — повсюдно поширені камери відеоспостереження, металопшукачі в школах, перевірка багажу в аеропортах, куленепробивні каси в банках, системи безпеки в будинках і підприємствах. Також слід звернути увагу на використання засобів індивідуального захисту (шокери, булави, рятувальні шнури/механізми виклику екстреної допомоги) та систем блокування запалювання з пристроями алкогольного датчика для запобігання запуску автомобіля в стані алкогольного сп'яніння. Можна також визначити апаратні технологічні інновації, які використовуються поліцією, включаючи нову зброю, пристрої менш нелетальної сили, нові технологічні патрульні автомобілі та нове поліцейське захисне спорядження.

За останні роки було розроблено широкий спектр нових м'яких технологічних інновацій, які використовуються як інструмент запобігання злочинності. Останні технологічні інновації включають інструменти класифікації ризиків правопорушників останнього покоління, появу протоколів оцінки загроз, інструментів ідентифікації знущань, програмне забезпечення, розроблене для запобігання крадіжці особистих даних, нові інструменти для моніторингу розташування та переміщення груп ризику, таких як психічно хворі правопорушники та сексуальні злочинці, а останнім часом нові інструменти оцінки, призначені для виявлення осіб, які, ймовірно, є злочинцями (або жертвами) вбивства в межах зазначений термін.

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Анастасія МІРОШНІЧЕНКО

Харківський національний університет внутрішніх справ

ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ КОНФЕРЕНЦІЙ ЯК НОВІ НАВИЧКИ В СУДОВОМУ ПРОЦЕСІ

Хоча відеодзвінки не були новинкою, коли вразив COVID, широке використання Microsoft Teams, Zoom та інших технологій відеоконференцій як в юридичних фірмах, так і з клієнтами вибухнуло через пандемію, змушуючи всіх працювати з дому. На додаток до зустрічей, судові засідання перемістилися в Інтернет, і навіть гучні випробування відбувалися через Zoom. Оскільки суди впроваджують програмне забезпечення для віртуальних слухань, як-от CaseLines, тенденція віртуальних слухань, безсумнівно, переживе пандемію та вимагатиме нових навичок від суддів. Адвокатура вимагає від адвокатів бути підготовленими, добре організованими, мати гарні матеріали, бути ввічливими та ввічливими, але, що не дивно, існують додаткові фактори, які слід враховувати для віртуальних слухань та медіації.

Перше міркування — це визначити «свої наміри щодо віртуальної взаємодії, будь то арбітраж чи посередництво», — каже Робін Додокін, юрист, посередник і арбітр Dodokin Law & Conflict Resolution в Торонто. «Дуже легко відчувати, що це просто конференц-дзвінок, і бути занадто невимушеним», — каже вона; але «ви повинні включитися в слухання або посередництво, навіть якщо ви працюєте над кухонним столом».

Особливу увагу потрібно приділяти взаємодії з іншими сторонами, «оскільки вони набагато інтимніші» у віртуальному середовищі, каже вона. Якщо, наприклад, хтось використовує два монітори і дивиться від камери на документи, «може здатися, що ви не звертаєте уваги». І якщо ваше обличчя занадто близько до камери, «це не схоже на зал суду. Усе збільшується тим фактом, що ми практично один одному в обличчя».

Віртуальне провадження може покращити доступ до правосуддя у цивільних справах кількома способами: сторонам не доведеться їздити на слухання і, можливо, менше часу відлучатися від роботи, що економить час; занепокоєння щодо фізичної доступності судів і будівель не є проблемою; технологія доступна кожному, хто має розумний пристрій; деякі витрати можуть бути зменшені, оскільки питання планування та ведення справ можна вирішувати практично та швидко без участі сторони чи адвоката в суді; можливі деякі інші скорочення витрат на віртуальні процедури; наприклад, немає витрат на оренду кімнати чи проїзд для свідків; це дозволило вирішувати суперечки ефективно та безпечно під час пандемії.

Віртуальні процедури продовжуватимуть використовуватися після пандемії та, можливо, з використанням гібридного процесу віртуального та особистого. Ймовірно, буде більше заявок на віртуальні процедури через їх переваги, і особливо на міжнародний арбітраж, де є сторони та експерти в країнах по всьому світу.

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Дмитро НАЗАРЕНКО

Харківський національний університет внутрішніх справ

АМЕРИКАНСЬКІ ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ

Найкращий спосіб боротьби зі злочинністю – це запобігти її появі, а технології є на передньому краї запобігання злочинам. Знову ж таки, інструменти штучного інтелекту та прогнозна аналітика з використанням великих даних є ключовими для встановлення зв'язків, які можуть зупинити злочин до його початку, але правоохоронні органи також використовують у своїй роботі інші інструменти.

У Чикаго поліцейські використовують технологію ShotSpotter, яка триангулює інформацію, щоб визначити точне місце пострілів. Поєднання цієї інформації з технологією виявлення номерних знаків полегшує поліцейським керувати патрулюваннями в районах із високим рівнем злочинності та розслідувати стрілянини. У південному передмісті запустили систему виявлення вогнепальної зброї, яка використовується в Чикаго та інших великих містах, яка в режимі реального часу повідомляє поліцію про місце обстрілу. Calumet City оголосив про розгортання ShotSpotter, технології, яка використовує стратегічно розміщені акустичні датчики для точного визначення стрілянини та оповіщення поліції за лічені секунди про точне розташування цієї пострілу, кількість випущених стрільців і пострілів, а також тип зброї, що стріляє. Каліфорнійська компанія, яка має контракти з десятками міст по всій країні, не гарантує, що її технологія зменшить насильство з використанням зброї, але виставляє рахунок як інструмент для боротьби зі злочинністю, який підвищує безпеку офіцерів і допомагає поліцейським розслідуванням, полегшуючи швидке реагування на інциденти зі стріляниною, про які інакше можна було б не повідомити владу.

Технологія розпізнавання облич також є важливою для боротьби зі злочинністю. Правоохоронні органи використовували розпізнавання

облич на великих заходах, наприклад, щоб ідентифікувати осіб, яких розшукують за злочини, порівнюючи їхні обличчя з базою даних сотень тисяч відомих правопорушників. А на кордоні прикордонники США використовують сенсорні технології для оцінки фізичної та психологічної поведінки, щоб визначити, чи можуть люди в'їхати в країну з підступними цілями. Технологічна революція в поліцейській діяльності розгортається у великих містах і малих громадах по всій країні, оскільки все більше поліцейських відділів купують програмне забезпечення для розпізнавання облич. Завдяки штучному інтелекту система розпізнавання облич дозволяє офіцерам надсилати зображення облич людей, зроблені в польових умовах або зняті з фотографій чи відео, і миттєво порівнювати їх із фотографіями в державних базах даних — фото, записи в тюрмах, водійські права.

Усі ці технології розроблені з єдиною метою запобігання злочинності, і ми бачимо лише верхівку айсберга, коли справа доходить до цих інструментів.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Юлія НЕЖУРІНА

Харківський національний університет внутрішніх справ

МАЙБУТНІ ПЕРСПЕКТИВИ ПОЛІЦІЇ

Нові технології, нові методи та нові ідеї внесли значні зміни в правоохоронні органи. Поліція та правоохоронні органи по всій країні сприяють змінам, впроваджуючи творчі ідеї, адаптуючись до мінливих умов та враховуючи думки офіцерів та партнерів з громади. Інновації, які формують майбутнє правоохоронних органів, починаються з нових технологій, які підтримують нові концепції операцій, забезпечуючи втручання та відносини, які забезпечують безпеку суспільства. Правоохоронні органи дбають про безпеку суспільства. Тому не дивно, що змінилося суспільство, змінилися й правоохоронні органи. Нові технології, нові методи та нові ідеї суттєво змінили професію. Але за своєю суттю правоохоронні органи вимагають такої ж самовідданості громадам, такого ж почуття обов'язку та самопожертви, та такої ж чесності, якою вона завжди володіє.

Сьогодні темпи розвитку технологій прискорюються швидше, ніж будь-коли. Нові пристрої та сервіси з'являються щодня. Тепер ми можемо замовити все, де завгодно — від програмного забезпечення до поїздки від абсолютно незнайомої людини — використовуючи лише

телефон. Ми можемо охопити будь-кого або мільйони людей миттєво. Наша здатність вчитися і робити добро, а також здатність деяких завдавати шкоди є більшою, ніж будь-коли. Технології змінюють основні аспекти того, як ми взаємодіємо як суспільство, і в міру того, як змінюється суспільство, також змінюватимуться інструменти, методи та концепції, які чоловіки та жінки з правоохоронних органів використовують для забезпечення нашої безпеки.

Інновації – це не лише новітні гаджети, а й пошук нових способів покращити ситуацію. Інновації можуть мати форму нових концепцій, нових методів або нових інструментів. Але інновації, як правило, працюють найкраще, коли всі ці форми об'єднуються, щоб поліція та правоохоронні органи могли мати більше розуміння та вплив, ніж будь-коли раніше. Інновації, які формують майбутнє правоохоронних органів, починаються з нових технологій, які підтримують нові концепції операцій, уможливають втручання та відносини, які забезпечують безпеку суспільства.

І хоча технології, методи та інструменти можуть продовжувати розвиватися, суть правоохоронних органів залишається незмінною: невтомна робота над покращенням залучення громади та громадської безпеки. Інновації, ймовірно, принесуть більше розуміння та безпеки, ніж будь-коли раніше, але той самий професіоналізм і дисципліна, які принесли правоохоронним органам минуле століття, залишається ключем до успіху в наступному.

*Консультант з мови **В. В. Кочина***

УДК 351.74:001.895](100)(06)

Тетяна НЕСКРЕБА

Харківський національний університет внутрішніх справ

НАГРУДНІ ВІДЕОРЕЄСТРАТОРИ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Прихильники відеореєстраторів стверджують, що вони захищають поліціантів від неправдивих звинувачень, зменшують відповідальність правоохоронного органу та скарг громадян, а також надають докази для використання в суді. Протягом останніх років правоохоронні органи експериментують із використанням відеореєстраторів. На відміну від камер, встановлених на транспортних засобах, відеореєстратори рухаються разом із поліціантами, коли той відходить від патрульної машини. Відеореєстратори можна прикріпити до кишені сорочки, шолома, окулярів або значка, а також вони можуть служити доповненням

автомобільних відеосистем або забезпечити додатковий варіант дорогим автомобільним системам, які деякі відділи не можуть собі дозволити.

В Сан-Матео (Каліфорнія) з населенням приблизно 98000 осіб розташованим приблизно у 20 милях на південь від Сан-Франциско, поблизу Кремнієвої долини, працюють численні високотехнологічні компанії. В управлінні поліції 100 поліціантів. Близькість до технологічного анклаву добре послужила управлінню поліції, надаючи йому можливість бути полігоном для тестування нових технологій, таких як мережа WiFi, що надає поліціантам бездротовий широкосмуговий доступ до баз даних правоохоронних органів.

За останні роки управління поліції провело п'ять пілотних випробувань відеореєстраторів і вирішило не використовувати їх, хоча відеореєстратори надзвичайно важливі для правоохоронців.

Поліціанти виявили, що жоден із відеореєстраторів не підходить для постійного носіння, тому що камери бачать не те, що потрібно правоохоронцю. Якщо камера встановлена на шоломі, тоді вона працює добре.

Системи розпізнавання автомобільних номерів мають інтегровану технологію. Відеореєстратори, які у майбутньому будуть носити поліціанти можуть включати такі системи, а також програмне забезпечення для розпізнавання обличчя та сканування навколишнього середовища.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Богдана НЕШТА

Харківський національний університет внутрішніх справ

ЦИФРОВА ТРАНСФОРМАЦІЯ У ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ

Швидкий розвиток сучасних технологій та засобів зв'язку відкриває нові можливості для вчинення кримінально-караних діянь. Сфера діяльності злочинців широка: від шахрайства в інтернеті, фішингу, викрадення особистих даних, відстеження даних до небезпечного комп'ютерного саботажу.

Величезна цифрова база даних стала викликом для силових структур. Перед працівниками поліції стоїть непросте завдання, яке полягає в пошуку слідів та доказів злочинно значущих дій у мережах інформаційно-комунікаційних технологій. Цифрові сліди в комп'ютерах, пристроях зв'язку та мережах відіграють все більшу роль у слідчих провадженнях.

Використання сучасних інформаційно-комунікаційних технологій стало звичним явищем у повсякденній роботі поліції. Роботу в Федеральному управлінні кримінальної поліції і німецькій поліції на сьогодні важко уявити без функціонуючої ІТ-інфраструктури.

Використовується весь спектр інформаційних технологій: від розробки спеціального програмного забезпечення для потреб поліції до великих даних і міжнародних мережевих ІТ-систем. Високоавтоматизовані мережеві та інтелектуальні системи, засновані на оцифровці, робототехніці, сенсорних датчиках, а також кіберфізичних системах і великих даних, суттєво змінюють усі сфери робочого середовища поліції. Цифрова трансформація все частіше використовується в технології роботи поліції на місці злочину.

Відділ ІТ-криміналістики, як центральний сервісний підрозділ Федерального управління кримінальної поліції, підтримує розслідування у збереженні доказів з носіїв даних та готує їх до криміналістичного аналізу. Метою діяльності сервісного центру є сприяння превентивній діяльності, наприклад, надання консультацій щодо можливих технічних превентивних заходів, а також підтримка поліцейських розслідувань на високому технічному рівні. Технології, розроблені шляхом систематичного та безперервного спостереження, аналізуються на предмет їхньої актуальності для поліції, а в особливих випадках також тестуються. «Якщо ми хочемо ефективно боротися зі злочинністю, ми повинні прагнути візуалізувати майбутнє, щоб зробити обґрунтовану оцінку ризику. Це вимагає всебічного раннього виявлення та раннього розслідування». (Йорг Цірке, головний комісар Федерального управління кримінальної поліції.)

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Олег ОБЕРНІХІН

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ РОБОТОТЕХНІКИ ПОЛІЦІЄЮ СПОЛУЧЕНИХ ШТАТІВ

Роботизація щодня проникає в різні сфери життя. Роботи можуть швидко виконувати занадто небезпечні, складні чи трудомісткі речі. Робототехніка користується великим попитом у поліції США. Дрони, прилади зору, роботи-сапери, патрульні роботи полегшують роботу поліції, роблять її безпечною для більшості поліцейських та дозволяють контролювати більше територій. Департамент поліції Нью-Йорка

використовує Digidog - роботизованих собак від Boston Dynamics, хоча він все ще перебуває в тестовому режимі. Планується, що їх використовуватимуть у небезпечних ситуаціях, коли є ризик для життя поліцейських. Серед заявлених переваг Digidog – можливість бачити в темряві та оцінювати, наскільки безпечно для поліцейського проникнути в приміщення. Поліція вже використовувала Digidog на практиці – наприклад, для звільнення заручників. Крім камер, роботи оснащені динаміками та мікрофоном, щоб офіцери могли використовувати їх для переговорів із злочинцями. У поліції впевнені, що завдяки Digidog кількість постраждалих та загиблих працівників має зменшитися. Хоча є побоювання, що таких роботів, як і будь-який пристрій, можна зламати та використати для шкоди – наприклад, несанкціонованого збору інформації про людей. За словами Майкла Перрі, віце-президента з розвитку бізнесу Boston Dynamics, компанія серйозно ставить до захисту від несанкціонованого доступу, а самі роботи не задумувалися як приховані інструменти масового спостереження, оскільки вони шумні та мають багато миготливих індикаторів. Knightscope створює футуристичних автономних роботів, призначених для безпеки під час патрулювання торгових центрів та інших громадських місць. Також компанія оголосила про можливість розпізнавання обличчя. У разі виявлення підозрілих осіб або злочинців здійснюється дзвінок на гарячу лінію. Сучасні технології поступово об'єднують людей і розумні машини в одну велику мережу соціального апарату, тому нам необхідно набути навичок управління ними та поводження з ними.

Консультант з мови **Н. В. Краснова**

УДК 351.74:001.895](100)(06)

Валерія ОСТАПЕНКО

Харківський національний університет внутрішніх справ

ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ОБЛИЧЬ (FR). БІОМЕТРИКА

У поліції вже давно використовують біометричні дані, в першу чергу відбитки пальців для ідентифікації. Але зараз багато хто використовує портативні сканери та технологію розпізнавання обличчя, щоб підвищити швидкість і точність ідентифікації. За даними PoliceOne, хоча ці технології є новими, вони є більш поширеними, ніж ми думаємо: одне з двох дорослих американських облич є в мережі розпізнавання облич правоохоронних органів. Ця 117-мільйонна бібліотека облич, яку розміщує ФБР, може допомогти офіцерам знайти людей на місці або порівняти фотографії. Однак доступність цієї інформації викликає певні

проблеми з конфіденційністю. Тож правоохоронні органи обережно підходять до цієї технології.

Голова Чафетц, член рейтингу Каммінгс, член комітету, розповідає про використання Федеральним бюро розслідувань (ФБР) технології розпізнавання облич (FR). Наступні програми ФБР використовують технологію FR для правоохоронних цілей. Це: 1) система ідентифікації нового покоління (NGI) ФБР, розташована в відділі інформаційних служб кримінального правосуддя (CJIS) ФБР, і 2) відділ послуг з аналізу, порівняння та оцінки обличчя (FACE), також розташований у відділі FBI CJIS.

1. NGI підтримує сховище фотографій, відоме як міждержавна фотосистема (IPS). Усі фотографії пов'язані з відбитками десяти відбитків пальців і кримінальним минулим. NGI-IPS дозволяє автоматично здійснювати пошук FR уповноваженими місцевими, державними, плеємними та федеральними правоохоронними органами. Правоохоронний орган подає на обшук сховище фотографій «дослідницьку» фотографію, отриману в результаті уповноваженого правоохоронного розслідування. NGI-IPS повертає галерею фотографій «кандидатів» із 2-50 особами (за умовчанням 20). Після цього правоохоронні органи повинні вручну переглянути фотографії кандидатів і провести подальше розслідування, щоб визначити, чи є на фотографіях кандидатів та сама людина, що й фото зонда. Технологія NGI-IPS використовується лише як слідча, а не як засіб позитивної ідентифікації. Посібник із впровадження політики NGI-IPS став доступним для авторизованих користувачів правоохоронних органів, які отримують фотографії кандидатів із системи ідентифікації наступного покоління міждержавних фотографій. У політиці зазначено, що фотографії не надаються як позитивна ідентифікація та не можуть служити єдиною підставою для дій правоохоронних органів. Крім того, ФБР оприлюднило політику та процедури, які пред'являють юридичні, політичні та безпекові вимоги до правоохоронних користувачів NGI-IPS, включаючи заборону надсилати фотографії зонда, отримані з порушенням Першої або Четвертої поправок. Важливо відзначити, що ФБР не зберігає фотографії зонду; зонди шукають і видаляють. Таким чином, NGI-IPS залишається сховищем виключно фотографій, які добровільно надсилаються з відбитками пальців під час арешту.

2. Підрозділ FACE Services надає провідну підтримку польових офісів ФБР, оперативних відділів і юридичних аташе, порівнюючи зображення облич осіб, пов'язаних із відкритими оцінками² та активними розслідуваннями³, із зображеннями облич, доступними в державних і федеральних системах FR. У обмежених випадках відділ

обслуговування FACE надає підтримку FR у закритих справах ФБР (наприклад, про зниклих безвісти та розшукуваних особах) і може запропонувати підтримку в розпізнаванні федеральних партнерів. Підрозділ служби FACE приймає лише «зондові» фотографії, які були зібрані відповідно до відповідних юридичних органів у рамках санкціонованого розслідування ФБР. Отримавши фотографії, відділ служби FACE шукає їх за допомогою програмного забезпечення FR у базах даних, дозволених для використання ФБР, що призводить до створення фотогалереї потенційних кандидатів. Підрозділ служби FACE виконує ручне порівняння фотографій кандидатів із фотографіями зонда, щоб визначити цінність кандидата як керівника розслідування. Ця послуга НЕ забезпечує позитивну ідентифікацію, а скоріше, слідство та аналіз, щоб підтвердити цю інформацію.

Використовуючи автоматизовану технологію FR для пошуку зображень у галереї, як описано для NGI, ФБР також використовує автоматизований FR як спосіб упорядкування або «сортування» файлів цифрових зображень, які були отримані згідно з уповноваженим розслідуванням правоохоронних органів.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Анастасія ОЩЕПКОВА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВООХОРОННИХ ОРГАНІВ США

Інноваційні технології – радикально нові чи вдосконалені технології, які істотно покращують умови виробництва або виявляються товаром. Зазвичай вони мають знижену капіталомісткість, характеризуються більшою екологічністю та меншими потребами в енергії.

У наш час, швидкого технічного розвитку інноваційні технології просто необхідні в органах поліції. Вони допомагають боротися зі злочинністю та новими категоріями правопорушень. В цій роботі ми розповімо про інноваційні технології на службі правоохоронних органів США.

Від дронів і камер на тілі до програмного забезпечення для розпізнавання обличчя та штучного інтелекту, ось список найважливіших технологій, які надають правоохоронним органам нові способи захисту та підтримки.

Програмне забезпечення для розпізнавання обличчя.

Одна з найбільш суперечливих нових поліцейських технологій є використання програмного забезпечення для розпізнавання обличч. Коли цей інструмент уперше увійшов до репертуару правоохоронних органів, багато хто був стурбований тим, що він буде використовуватися неетично та може порушити права людини. Але, на щастя, цього не сталося, і розпізнавання обличчя виявилось ефективним інструментом в ході розслідування.

Метою програмного забезпечення для розпізнавання обличчя є те, що воно допомагає підвищити безпеку в ряді випадків. Співробітники поліції Нью-Йорка змогли виявити та заарештувати підозрюваного у зґвалтуванні протягом 24 годин після нападу за допомогою програмного забезпечення для розпізнавання обличчя. І оскільки розпізнавання обличчя дуже багатообіцяюче, Міністерство внутрішньої безпеки США прогнозує, що до 2023 року воно буде використовуватися в 97% випадків.

Роботи.

Багато правоохоронних органів сьогодні використовують роботизовані камери нового покоління для візуального та звукового спостереження за потенційними місцями злочину, які можуть бути надто небезпечними або важкодоступними для працівників. Деякі з цих пристроїв, навіть "метані" (до 120 футів і здатні витримати кілька падінь з висоти 30 футів), працюють на електродвигуні та оснащені високотехнологічними колесами, які дозволяють їм переміщатися, підніматися та досліджувати навіть найважчі місця за допомогою бездротового доступу та керування навченого офіцера.

Автомобільний виробник Ford подав патент на поліцейську безпілотну машину, оснащену штучним інтелектом. Ці високотехнологічні крейсери розроблені для того, щоб ловити порушників правил дорожнього руху або водіїв з обмеженими фізичними можливостями шляхом передачі інформації співробітникам або перевозячи додаткового пасажирів, який може провести арешт.

Покращені камери для носіння на тілі.

Відео з поліцейськими, які виконують свою роботу в складних ситуаціях, було рідкістю, але сьогодні воно повсюдно. За допомогою камер, які надягають на тіло, зросла здатність правоохоронців та громадськості отримати уявлення про поліцію на рівні вулиці.

Крім того, завдяки постійним удосконаленням технологій, такі камери виробляють менш громіздкими та більш міцними, а деякі натільні камери розроблені для кращої інтеграції з автомобільними системами, щоб забезпечити синхронізацію відеоподій з різних точок зору. Інші досягнення включають вищу роздільну здатність, чистіший звук, ширші поля зору та підвищену стійкість до умов навколишнього середовища, таких як екстремальний холод.

Значним прогресом також можна вважати «розумні» кобури, які призначені для активації камери тіла в будь-який момент, коли офіцер дістає зброю. Принаймні один виробник натільних поліцейських камер випустив камеру, здатну подавати сигнал тривоги, коли поліцейський падає. Найближчим часом – камери для носіння на тілі, оснащені функцією розпізнавання обличчя.

Науковий керівник А. В. Білоусов

УДК351.74:001.895](100)(06)

Станіслав ПАВЛЕНКО

Харківський національний університет внутрішніх справ

ДРОНИ НА СЛУЖБІ ПРАВОПОРЯДКУ

Світ розвивається з неймовірною швидкістю, кожного дня з'являються нові технології, які допомагають в роботі як правоохоронним органам, так і зловмисникам. Саме тому поліція має йти в ногу з сучасним світом та переймати інновації, які зазнали успіху в зарубіжних країнах.

Гарним прикладом є досвід Японії з використанням безпілотних дронів для викриття та попередження протиправних дій:

- дрони із сіткою використовуються для визначення безпілотників, які залітають у недозволені місця, де знаходяться незаконні предмети або речовини, а також для перехоплення дронів, які використовуються для терористичних актів;

- спостереження за певними особами, переслідування та відео фіксація дій, вчиняємих ними;

- патрулювання вулиць; спеціаліст, який керує дронами, може, не виходячи з кабінету, слідкувати за діями оточуючих з повітря об'єктів, та одразу фіксувати скоєння правопорушення;

- припинення випадків браконьєрства; обладнаний термографічною камерою дрон на відстані кілометра може визначити точне місцезнаходження осіб навіть у нічний час;

- дрони допомагають у пошуку зниклих людей; маючи велику швидкість та огляд з повітря, вони є дуже ефективними – одного дрону достатньо, щоб охопити величезну територію.

Ефективність дронів у правоохоронній службі очевидна. У США, протягом 2020 року застосування дронів було таким:

93 правоохоронні органи штату Мінесота використовували безпілотники 1171 раз – із сукупною ціною майже 1 мільйон доларів. Майже половина (506) були лише з метою «підготовки офіцерів». Інші

види використання включали збір інформації на основі обґрунтованої підозри у невизначених злочинах (185), запити інших державних органів, не пов'язаних із правоохоронними органами (41), розслідування дорожньо-транспортних пригод (39), а також підготовку та моніторинг публічних заходів (6 і 12 відповідно).

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Владислав ПИЛИПЧУК

Харківський національний університет внутрішніх справ

ІНОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВОПОРЯДКУ

Етика цифрових технологій в поліції. Широке використання цифрових технологій в судовій і правоохоронній діяльності супроводжується великою етичною проблемою. Використання сучасних технологій правоохоронними органами відкриває нові можливості для забезпечення безпеки громадян, але створює загрозу правам і свободам.

Цифрові технології в роботі поліції. Щоб ефективно боротися як з традиційною, так і з кіберзлочинністю, правоохоронні органи повинні йти на крок попереду правопорушників у використанні технічних досягнень. Перевагою поліції залишається збір і обробка величезного обсягу даних. У той же час на перший план виходить прогностична поліцейська діяльність.

На Заході поліцейські служби та судові органи активно розвивають і використовують окремі елементи цифровізації та цілі системи штучного інтелекту. За даними Інтерполу і Європолу, співробітники поліції більш ніж в 70 країнах використовують різні види прогностичної аналітики на практиці.

Основні напрямки використання цифрових технологій в поліцейській діяльності:

- удосконалення поліцейських баз даних;
- прогностна аналітика для оцінки ймовірності вчинення злочину на певній території;
- використання роботів для патрулювання;
- пошук та ідентифікація зниклих безвісти людей;
- контроль якості роботи поліції;
- боротьба з корупцією;

На замовлення Європейського Союзу міжнародна група вчених розробила і в 2013 році запустила систему ePOOLICE (Раннє

розпізнавання загроз організованої злочинності на основі сканування інформаційного середовища). Щоб знайти ознаки організованої злочинної діяльності та оцінити ризик вчинення злочину система сканує сторінки веб-сайтів, електронну переписку та поліцейську інформацію.

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Вікторія ПІДГАЙНА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ

Важливим елементом Нацполіції є поглиблення співпраці з активними громадянами. Адже ефективна охорона громадського порядку неможлива без активної участі громадян, зацікавлених у безпеці. У сучасному світі розробляються певні інноваційні технології для подальшої роботи. Одна з них уже впроваджена. Наприклад, патрульна поліція може їздити на електричному скутері. Завдання патрульних передусім превентивне – зокрема, пояснити, як правильно поводитися на цьому виді транспорту. Також інспектори зможуть швидше реагувати на виклики.

Інший приклад – можливість запровадження офіційної відеозйомки або покращення запису наданої інформації. Цей метод полегшить боротьбу з тими, хто хоче уникнути відповідальності, а також фіксувати всі дії правопорушника. Було б дійсно ефективно, щоб цей процес відбувався набагато швидше.

Прикладом іноземних винахідників, який би допоміг у боротьбі з злочинцями – інтернет тіл. Йдеться про гаджети і додатки, які мають функцію моніторизувати різні показники людського тіла, але й до того ж самостійно коригуватимуть показники та вносити поправки. Пристрої підключатимуться до мозку, що забезпечить з'єднання того, що відбувається в реальному часі з віддаленими комп'ютерами, куди надходитимуть дані про роботу в організмі. Крім моніторингу здоров'я, це може і підвищити кібербезпеку, розглядаючи стан людини.

Приблизно принаймні такі принципи роботи його покращили. Тому я вважаю, що можна розвивати набагато більше інноваційних технологій, але якби ми вдосконалили одну із запропонованих – було б набагато краще.

Важливо пам'ятати, що інноваційні технології не лише покращують та полегшують роботу поліції, а й покращують боротьбу зі злочинністю.

Науковий керівник Н. Л. Горбач

УДК 351.74:001.895](100)(06)

Владислав ПОЛТАВСЬКИЙ

Харківський національний університет внутрішніх справ

ЯК НАТІЛЬНІ КАМЕРИ МОЖУТЬ ДОПОМОГТИ ПОЛІЦІЇ

Оскільки технології продовжують розвиватися, правоохоронним органам доводиться не відставати. Агентства всіх рівнів інвестують у новітні та найкращі технології, щоб краще обслуговувати та захищати своїх офіцерів та громад.

Натільні камери були чудовим доповненням для багатьох правоохоронних органів по всій Сполучених Штатах. Хоча є негативні аспекти цієї технології, про які поліцейські повинні знати, натільні камери вже виявилися корисними в багатьох випадках по всій країні. Протягом останнього десятиліття використання смертельної сили поліцією стало предметом розмови. Завдяки нескінченному циклу новин і поширеності соціальних мереж, ці ситуації можуть швидко вийти з-під контролю, перш ніж будь-які факти будуть виявлені. Натільні камери – це технологія, яка допомогла громадськості отримати місце в першому ряду, щоб побачити, що бачить поліція та як вона реагує.

Наприклад, у Клівленді, штат Огайо, чотирьох поліцейських судили за випадок застосування смертельної сили. Завдяки записам натільних камер, громадськість могла почути та побачити дії цих офіцерів і вирішити, чи були їхні дії виправданими. Після вбивств Джорджа Флойда, Бреонни Тейлор та незліченної кількості інших чорношкірих життів від рук поліції, постраждалих сімей та громадських груп, прихильники реформ поліції, законодавці та навіть поліцейські департаменти закликають правоохоронні органи прийняти та розширити програми натільних камер. Цей дзвінок не новий. Натільні камери були запропоновані як інструмент підзвітності поліції після вбивств Майкла Брауна та Еріка Гарнера в 2014 році. Їх закликали після вбивства поліцією Філандо Кастилі в 2017 році, і сьогодні їх знову закликають, оскільки поліція продовжує жорстоко порушувати життя чорношкірих. і використовувати надмірну силу щодо протестувальників, які виступають за расову справедливість.

Натільні камери можуть служити скоріше інструментом для спостереження за цивільним населенням і послаблення прав людей, ніж для притягнення офіцерів до відповідальності. Оскільки натільні камери можуть переміщатися як у громадських, так і в приватних місцях, вони фіксують величезну кількість даних про людей, крім тих, хто взаємодіє з поліцейським, який носить камеру.

Ті, хто закликає встановити камери, розглядають цю технологію як інструмент для кращого контролю поведінки офіцера. Деякі прихильники сподіваються, що камери зменшать неналежну поведінку та підвищать відповідальність поліції. У деяких випадках кадри з камери проливають світло на неправомірну поведінку поліції, яку інакше не було б видно.

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Дарина **ПРИХІДЬКО**

Харківський національний університет внутрішніх справ

НОВІТНІ ТЕХНОЛОГІЇ ДЛЯ ПОПЕРЕДЖЕННЯ ТЕРОРИСТИЧНИХ ЗАГРОЗ

Завдяки технологічному прогресу світ наповнюється обладнанням, яким цікавляться як терористи, так і ті, хто з ними борються. Терористи все частіше використовують сучасні технології з поганими намірами. Наука та технології, що спеціалізуються на боротьбі з тероризмом, включають засоби забезпечення передчасного підриву вибухових речовин або гальмування спрацьовування вибухових речовин. Більшість науково-технічних засобів боротьби з тероризмом дуже корисні для охорони здоров'я, правоохоронних органів або розвідувальних цілей.

Технології безпеки дозволяють у режимі реального часу ідентифікувати, локалізувати та спланувати терористичні наміри шляхом прогнозування ймовірних ризиків. Вони також дають змогу націлюватись на мобільність, комунікації, фінансові та банківські операції терористів. Біометрія є однією з цих технологій з численними додатками, включаючи сканування ДНК, райдужної оболонки та сітківки ока, розпізнавання обличчя та навіть емоційного розпізнавання.

Спостереження полягає в нагляді, зборі, запису та обробці інформації, що стосується окремих переміщень, маршрутів, поведінки та комунікацій для визначення ймовірного ступеня ризику.

Технологія також сприяє ідентифікації та знаходженню невлених терористів за допомогою прогнозного штучного інтелекту. На основі аналізу даних (видобутку даних з великих взаємопов'язаних баз даних), технології прогнозування використовують математичні моделі.

Дрони служать для відеоспостереження та дистанційної ліквідації терористів, а також як засіб розвідки маршрутів і місць нападу, моніторингу діяльності в режимі реального часу або як саморобні вибухові пристрої (в повітрі, воді чи на землі).

Науковий керівник **Л. С. Сазанова**

УДК 351.74:001.895](100)(06)

Ростислав ПРОКОПЕНКО

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ НОВИХ ТЕХНОЛОГІЙ У ПОЛІЦІЇ

З роками з'явилося багато інших нових технологій, від автомобільних ноутбуків і бронезилетів до нових технологій, таких як смартфони та камери для носіння на тілі. Простіше кажучи, технології та поліція йдуть рука об руку. І це добре, особливо коли ця технологія робить речі безпечнішими як для офіцерів, так і для тих, кому вони служать. Оскільки нові технології неминуче розвиваються, поліція має можливість використовувати їх для більшого блага у своїх відділах і громадах. Які найефективніші інструменти поліція вже використовує для забезпечення громадської безпеки?

Поліцейські дрони. Безпілотні літальні апарати або дрони, які використовуються військовими протягом багатьох років, стають все більш поширеними в правоохоронних органах. Багато відділів використовують їх для спостереження або збору доказів. Інші використовують їх для фотографування сцен аварій і навіть контролю над натовпом. Дрони також корисні для інших сфер правоохоронних органів, оскільки вони можуть стежити за виправними установами та відстежувати втікачів.

GPS. GPS також використовується поліцейськими відділами протягом багатьох років. Офіцери найчастіше використовували його для відстеження злочинців, але нещодавно GPS допоміг у моніторингу безпеки офіцерів. Нові розробки в технології GPS дають офіцерам більше інформації та деталей, ніж будь-коли раніше, забезпечуючи безпеку та ефективність на полі.

Офіцер - оператор супроводу (ціль). GPS дозволяє краще координувати та відстежувати, де знаходяться офіцери та транспортні засоби. Це може допомогти відділам ефективніше реагувати на інциденти. Це також дозволяє отримати точнішу інформацію про місцезнаходження для викликів, а також для більш безпечної та швидкої маршрутизації офіцерів до цих інцидентів.

Дартс переслідування автомобіля. Аварії, пов'язані з переслідуванням, щорічно отримують понад 55 000 поранень. Що якби ви могли відстежувати транспортні засоби в ситуаціях переслідування на відстані, забезпечуючи безпеку своїх офіцерів та інших водіїв на дорозі? Вони ще не надто поширені, але дротики переслідування транспортних засобів, як фізичний GPS в реальному часі, роблять саме це. Невеликий пінопластовий дротик, яким можна стріляти в

транспортний засіб, вони дозволяють офіцерам безпечно позначати, відстежувати та затримувати небезпечних осіб.

Виявлення пострілу. Виявлення вогнепальних пострілів не використовується багатьма відділами, але це може бути дуже корисним способом відстеження пострілів у певних областях. Використовуючи картографію та електронні датчики, виявлення вогнепальних пострілів дозволяє офіцерам негайно та точно реагувати. Деякі департаменти використовують виявлення вогнепальної зброї, щоб заповнити прогалини, виявляючи постріли, які не викликаються. «Ми виявили, що частота випадкових пострілів була для нас вражаючою», – розповідає ComputerWorld заступник комісара округу Нассау Вільям Фланеган. «Ще більше хвилювало, так це те, що нам не телефонували з цього приводу». Очевидно, що ця технологія корисна, але й дорога. Якщо у вашій місцевості спостерігається велика кількість обстрілів, можливо, це варто. Райони з рідкісними свідками також можуть вважати виявлення пострілів розумною інвестицією.

Однак корисно знати, що технології постійно розвиваються, і, ймовірно, ніколи не бракує можливостей для впровадження нових систем, які можуть додавати безпеку та ефективність кожному відділу.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Владислав РЕПАЛОВ

Харківський національний університет внутрішніх справ

ІННОВАЦІЇ ТА НАУКА ЯК ОСНОВА ВДОСКОНАЛЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Сьогодні наша країна продовжує формування сучасного, ефективного, якісного та дієвого механізму державних органів. Особливу роль в цьому механізмі відіграють органи правопорядку і, зокрема, поліція, на яку покладено обов'язок забезпечувати права і свободи громадян та охороняти встановлений порядок, не допускаючи протиправних посягань.

Незважаючи на зміни, система правоохоронних органів залишається недостатньо ефективною та закритою від суспільства. Для зміни даного становища поліцейським потрібно постійно розвиватися та вдосконалювати свої професійні навички, як фізично, так і духовно.

Існують різні способи розвитку професійних якостей, наприклад :

Участь у наукових семінарах та тренінгах;

Спілкування з громадянами, щоб підвищити рівень довіри населення.
Участь у різних проєктах, метою яких є розвиток особистісних якостей поліцейського.

Спілкування з іноземними колегами та перейняття досвіду;

Міжнародне партнерство на правоохоронних засадах

Прикладом такого партнерства для вдосконалення роботи правоохоронних органів є Фонд поліції (The National Police Foundation) створений у США – національна, позапартійна, некомерційна організація, яка займається вдосконаленням поліцейської діяльності за допомогою інновацій та науки.

Наразі ця організація співпрацює з сотнями поліцейських установ по всій Україні, а також на міжнародному рівні, забезпечуючи дослідження та переклади, навчання, технічну допомогу та впровадження сучасних технологій. Фонд є лідером у галузі безпеки та благополуччя офіцерів, охорони громадських служб, відкритих даних, розслідувань та технологій безпеки. Основна мета Фонду — сприяти підвищенню якості поліцейських послуг, щоб принести користь співробітникам та громадам, яким вони служать, а також зменшити рівень злочинності.

Консультант з мови Г. С. Бабак

УДК 351.74:001.895](100)(06)

Юлія РОГОЖИНА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ У РОБОТІ ПОЛІЦЕЙСЬКИХ

Нові технології, нові методи та нові ідеї принесли значні зміни в правоохоронні органи. Правоохоронні органи – це забезпечення безпеки суспільства. Тому не дивно, що, як змінилося суспільство, так само змінилися і правоохоронні органи. Нові технології, нові методи та нові ідеї принесли значні зміни в професію. Але за своєю суттю правоохоронні органи вимагають такої ж відданості громадам, того ж почуття обов'язку і жертви, і тієї ж цілісності, яка вона завжди має.

Розглянемо п'ять кращих інновацій в поліції, які формують майбутнє:

1. Об'єднання нових технологій для отримання більш швидкої обізнаності

Кожна слідча подорож починається зі збору фактів про світ. Традиційно ця робота була складною. Це може означати покладатися на пам'ять офіцера про номерний знак, щоб стежити за, або довгі години

пошуку потрібних частин інформації. Це часто означає бути там, бачити, чути і стримувати - і жоден відділ не може бути скрізь. Однак нові технології, такі як Інтернет речей (IP) і розумні датчики, можуть бути там, коли це необхідно.

Розумні датчики можуть бути використані для складання багатьох різних типів інформації, щоб допомогти офіцерам виконувати свою роботу швидше і ефективніше. Нові можливості можуть реєструвати місця, слухати постріли, потокове відео, прапори номерних знаків, сканувати бази даних, і йти на віртуальний патруль, що дозволяє офіцерам безпрецедентну обізнаність у своєму середовищі.

2. Використання цифрових технологій для підвищення безпеки офіцерів та громадян

Інтернет речей і розподілене зондування - це використання нових технологій для збору інформації про світ і вказувати в правильному напрямку. Що робити офіцерам на сцені? Розвиваються нові технології та практики, які можуть допомогти керувати діями у світі. Досягнення в таких областях, як зв'язок 5G, мініатюризація електроніки і доповнена реальність, дозволяють людям бачити, чути і діяти таким чином, що раніше було неможливо.

3. Використання баз даних для запобігання злочинності

Ми живемо у світі, переповненому даними. І оскільки багато відділів розгортають технологічні рішення, такі як доповнена реальність, камери тіла, зчитувачі номерних знаків і розумні датчики, вони, ймовірно, будуть генерувати більше даних щодня, ніж у всій своїй аналоговій історії. Успіх майбутніх стратегій правоохоронних органів залежить від можливості швидко та ефективно використовувати ці величезні обсяги даних для підтримки розслідувань та примусових дій. Але ці бази (гори) даних занадто великі для будь-якої людини, щоб прочесати, навіть якщо вони присвятили все життя пошуку.

Щоб отримати реальне розуміння, штучний інтелект (ШІ) і машинне навчання будуть ключем до майбутніх досліджень. Наприклад, щороку більше восьми мільйонів порад щодо місцезнаходження зниклих дітей повинна аналізувати команда з усього 25 слідчих. ШІ розгортається, щоб допомогти цим слідчим просіяти дані і знайти найбільш ймовірні приводи для ідентифікації експлуатованих дітей і возз'єднання їх з близькими. Штучний інтелект вже демонструє свою цінність у всьому світі, допомагаючи поліції Англії аналізувати відео з камер відеоспостереження, офіцери в Індії знаходять 3000 зниклих безвісти всього за чотири дні, а голландці знаходять багатообіцяючих потенційних клієнтів у холодних випадках.

4. Ретельне тестування того, що працює, і більш ретельний розгляд ключових ідей

Штучний інтелект і машинне навчання можуть допомогти знайти підказки, щоб націлити патруль або направити розслідування, використовуючи прості набори правил для перевірки нових гіпотез, визначення того, що працює, і масштабу успіхів. Подібний підхід - доказова поліція - також може бути застосований до методів самої поліцейської роботи. Доказова поліція включає в себе використання передових судово-медичних методів, щоб отримати більше інформації з тієї ж кількості доказів, але це також виходить за рамки цього, щоб вивчити серце діяльності поліції.

Поліція, заснована на доказах, може аналізувати дані про результати взаємодії поліції, щоб допомогти знайти найбільш ефективні методи та інструменти, мінімізуючи використання тактики, яка, як правило, погіршує ситуацію.¹⁰ В епоху, коли багатьох поліцейських просять робити все більше і більше з меншими ресурсами, поліція, заснована на доказах, прагне поєднати їх з зовнішньою допомогою, наприклад, академічні дослідники або програмісти, щоб допомогти зосередити свої зусилля на найбільш ефективній роботі поліції.

5. Створення міцніших локальних мереж для підвищення громадської безпеки

Місія правоохоронних органів - це безпека громади, а міцні відносини з громадою мають вирішальне значення для успіху кожної правоохоронної організації. Побудова тісних зв'язків у громаді стосується традиційної поліцейської допомоги та участі в місцевому рівні, але це також про використання інструментів, щоб допомогти людям безпосередньо повідомити про свої потреби та ризики. Нові технології можуть допомогти поліції розвивати свої зв'язки з громадою, дозволяючи офіцерам бути більш обізнаними та реагувати на потреби своїх виборців.

Наприклад, багато громад зараз використовують додатки, де громадяни можуть повідомляти поліції про незначні проблеми, такі як графіті або підозріла діяльність, надаючи поліції в режимі реального часу обізнаність, динамічну пріоритезацію дзвінків та свободу зосереджуватися на найактуальніших проблемах. Але людські стосунки не можуть управлятися тільки технологіями. Поєднання інноваційних підходів, таких як доказова поліція, може допомогти відновити ці відносини, змінивши способи і часи взаємодії офіцерів з населенням.

Зміни неминучі, але правоохоронні органи можуть зробити активні кроки для підготовки до майбутнього. Поряд з цими майбутніми тенденціями, зміна демографії змінює те, як буде виглядати офіцер майбутнього і як вони будуть проводити свій день. Керівництво правоохоронних органів має визнати ці зміни не тільки для набору

потрібного персоналу, але і для ефективного управління ними у світі, що переходить від цегли та розчину до бітів та байтів.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Артур РОЗУМ

Харківський національний університет внутрішніх справ

ЯК УДОСКОНАЛЮВАТИ РОБОТУ ПОЛІЦІЇ ЗА ДОПОМОГОЮ ІННОВАЦІЙ ТА НАУКИ

Завдяки розширеним електронним базам даних для ефективнішого використання ДНК та інших біометричних даних у правоохоронних органах, навіть використання відбитків пальців для ідентифікації підозрюваних стало високотехнологічним.

Наприклад, у звіті Сі-Ен-Бі-Сі (американський кабельний, супутниковий та інтернет телевізійний канал) пояснюється, як поліція Лондона тепер може використовувати мобільний біометричний пристрій INK, щоб сканувати відбитки пальців підозрюваного та в багатьох випадках встановити його особу протягом 60 секунд.

Поліційна патрульна машина схожа на мобільний командний центр, і це означає, що є багато комп'ютерів та приладів, якими поліціант може користуватися під час руху.

Однією з останніх інновацій, яка впроваджується в поліційні машини, є нова технологія голосових команд, що дозволяє поліціантам керувати багатьма функціями свого автомобіля під час руху та виконувати інші обов'язки з патрулювання.

Можливості цих голосових систем різні в різних поліційних машинах, але більшість з них можуть обробляти команди для пошуку номерного знака або включення сирени. Більш просунуті та найперспективніші можливості технології голосових команд у поліційних автомобілях значно полегшують подачу звітів – поліціанти можуть диктувати свої нотатки, які потім реєструються безпосередньо через систему віддаленого доступу до комп'ютера їхнього підрозділу.

Зараз багато підрозділів правоохоронних органів використовують роботизовані камери нового покоління для візуального та аудіоспостереження за потенційними місцями скоєння злочинів, які можуть бути занадто небезпечними або недоступними для поліціантів.

Деякі з цих пристроїв навіть витримують падіння (з 120 футів і можуть витримувати багаторазове падіння з 30 футів).

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Валерія РОМАНОВА

Харківський національний університет внутрішніх справ

ВАЖЛИВІСТЬ ЗБОРУ ДАНИХ ТА ІНФОРМАЦІЇ

Закони повинні наказати відповідним державним установам збирати кількісні дані, що стосуються насильства на основі «честі». Кількісні дані отримують шляхом вимірювання показників поширеності, реакції уряду та виконання програм. Ці дані можуть бути отримані державними органами статистики шляхом використання опитувань, проведених серед населення, а також шляхом отримання даних з відповідних адміністративних джерел, таких як лікарняні та поліцейські записи. Посібник з розробки системи статистики кримінального правосуддя містить розділ про віктимні дослідження, які враховують той факт, що багато злочинів можуть залишитися невідомими, а опитування щодо віктимізації та самозвітання допоможуть розкрити ці злочини. Особливо це стосується злочинів на честь честі, оскільки за оцінками багатьох експертів, фактична кількість таких злочинів значно перевищує кількість зареєстрованих випадків. Розробники законопроектів мають забезпечити, щоб закони вимагали збирання та розповсюдження статистичних даних, пов'язаних із «злочинами на честь честі», і створити базу даних для відстеження такої інформації. Органи влади повинні збирати дані щодо таких показників: форми насильства на основі «честі», частота, причини та фактори ризику, зв'язки між економічними позбавленнями та експлуатацією та насильством на основі «честі», коротко-, середні та тривалі- термінові наслідки, вплив на підгрупи жінок і дівчат, рівень судового переслідування, засудження, покарання, відносини між жертвою та злочинцем(ами), моделі віктимізації, включаючи повторну або багаторазову віктимізацію, етнічну приналежність, вік, стать, інвалідність, релігію, і використання зброї або небезпечних речовин.

Закони повинні виділяти достатнє державне фінансування для якісних досліджень, щоб краще зрозуміти причини, динаміку та наслідки злочинів «честь» та «честь» у відповідній країні. Якісні дані виходять за рамки статистичних даних, щоб забезпечити глибше, детальніше розуміння проблеми. Наприклад, Конвенція Ради Європи про запобігання та боротьбу з насильством щодо жінок і домашнім насильством закликає держави-учасниці підтримувати дослідження всіх форм насильства щодо жінок «з метою вивчення його першопричин і наслідків, випадків і частоти засуджених» (ст. 11(1)). Монітори повинні також оцінити існуюче законодавство, політику та програми щодо

запобігання насильству щодо жінок, переслідування насильницьких правопорушників та захисту постраждалих. Потім вони повинні проаналізувати, наскільки ці закони, протоколи та програми ефективні для забезпечення безпеки жертв та відповідальності правопорушників та запобігання насильству щодо жінок. Управління Верховної комісії ООН з прав людини випустило Навчальний посібник з моніторингу дотримання прав людини та Посібник для тренера, який містить рекомендації щодо моніторингу прав людини.

Хоча всі принципи, викладені в Навчальному посібнику ООН, є важливими, принцип не завдавати шкоди та збереження конфіденційності є надзвичайно важливим для захисту жертв та запобігання подальшій віктимізації чи заподіяння шкоди. Основним обов'язком особи, яка розшукує факти, є жертва або потенційні жертви порушень прав людини, і, як мінімум, особа, яка розшукує факти, повинна утримуватися від дій чи бездіяльності, які загрожують їх безпеці.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Богдан РОЩЕНКО

Харківський національний університет внутрішніх справ

ВАЖЛИВІСТЬ ЗБОРУ ВІДПОВІДНИХ ДАНИХ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИНАМИ

Грамотність даних – здатність отримувати значущу інформацію з даних – має бути метою кожного агентства. Багато відділів завантажують інформацію з диспетчерських систем САПР, завантажують інформацію з комп'ютерів поліцейських, встановлених на транспортних засобах, і надсилають інформацію по бездротовому зв'язку за допомогою машин для електронного цитування, не розуміючи, чому і як дані збираються. Розуміння «чому», що лежить в основі збору даних, допоможе заохотити, як збираються дані. Ціль ніколи не повинна полягати в тому, щоб збирати випадкові дані лише для того, щоб додати їх до пулу раніше зібраних даних – випадкові колекції даних призведуть до океану непридатних даних, таких як те, що ми маємо зараз. Метою завжди має бути збір даних для конкретної мети: боротьби зі злочинністю. Після того, як дані були зібрані з певною метою, тепер робота аналітиків та детективів у сфері злочинів полягає в тому, щоб перетворити ці дані в інформацію, а потім перетворити цю інформацію на розуміння.

Поліцейським органам потрібно більше відповідних даних і менше сміття, яке аналітики та детективи можуть швидко перетворити на

корисну інформацію. Справа в тому, що існує ТОНА даних. Правоохоронним органам потрібні розумні інструменти, щоб допомогти надати правильну/релевантну інформацію. На щастя, виправити нерелевантні звички збирання даних так само легко, як 1,2,3:

1. Числа представляють цікаву проблему для збирачів даних, оскільки їх можна легко транспонувати. Номери на VIN, номерні знаки, серійні номери та адреси повинні бути перевірені перед записом у будь-яке програмне забезпечення.

2. Особи: точний збір даних про людей також може становити проблему. Багато людей мають одне й те саме ім'я та прізвище, тому збирання відмінних характеристик так само важливо, як імена. В Арізоні, наприклад, 43 людини мають моє ім'я та прізвище; 4 мають однакове ім'я, по батькові та прізвище; і 1 – звільнений злочинець з насильством з іншого штату. Зверніть особливу увагу на особисту ідентифікаційну інформацію (PII), включаючи повне юридичне ім'я, точний номер соціального страхування, видимі татуювання та місце розташування татуювань, а також расу.

3. Помічники та друзі: Запишіть друзів та соратників, і ваш аналітик подякує вам пізніше! Завжди запитуйте у пасажирів зупинку і друзів вашого підозрюваного також їх ідентифікаційну інформацію. Просто пам'ятайте, що в більшості штатів пасажир на зупинках не повинні розмовляти з вами, якщо у вас немає порушення щодо цієї особи, але принаймні ви можете спробувати.

Як ви могли бачити, чим точніша інформація, тим легше буде її перетворити на розуміння. Великі дані потрібно зробити малими, щоб бути ефективними. Найкращий спосіб розпочати скорочення даних – це зрозуміти причину збирання, записувати точну інформацію та використовувати програмне забезпечення для аналізу, щоб перетворити дані на уявлення, щоб ви не залишилися плавати в океані даних, які не можна пити, бормочучи собі: «Дані, дані всюди але ні краплі не випити!»

*Консультант з мови **В. В. Кочина***

УДК 351.74:001.895](100)(06)

Дар'я РЯБЦЕВА

Харківський національний університет внутрішніх справ

РОБОТИ В РОБОТІ ПРАВООХОРОННИХ ОРГАНІВ

Для виконання різних завдань фахівці правоохоронних органів використовують технологію глобального позиціонування., зокрема

підтвердження присутності підозрюваних на місці злочину. Деякі роботи можуть навіть виконувати ті ж самі суворі завдання, які повинні виконувати офіцери, дозволяючи їм зосередитися на більш важливих справах.

Зараз велика кількість правоохоронних органів використовує роботизовані камери нового покоління для візуалізації та аудіоспостереження потенційних місць злочинів, які можуть бути занадто небезпечними або занадто важкими для офіцерів.

Деякі з цих пристроїв, які створені для «кидання» на відстань до 120 футів і здатні витримувати багаторазові 30-футові падіння, оснащені електродвигуном і оснащені високотехнологічними колесами, які дозволяють їм рухатися, підніматися та досліджувати навіть найскладніші приміщення під час бездротового керування кваліфікованим офіцером.

Автовиробник Ford подав патент на поліцейський безпілотний автомобіль, оснащений штучним інтелектом. Цей високотехнологічний крейсер розроблений для того, щоб ловити порушників правил дорожнього руху або водіїв з обмеженими фізичними можливостями шляхом передачі інформації співробітникам або перевозачи додаткового пасажирів.

Додаткові програми для використання роботів у поліцейській роботі, зараз і у найближчий час включають:

- збільшення можливостей роботів у зібранні інформації про спостереження, прийманні поліцейських звітів та забезпеченні комунікації в умовах, де безпека людей буде під загрозою.

- безперервна розробка Китаєм робота «AnBot» для патрулювання банків, аеропортів та шкіл

- патрулювання туристичних місцевостей за допомогою робота-офіцера з сенсорним екраном, який зараз застосовується в Дубаї.

Науковий керівник Л. І. Русанова

УДК [351.74: 001.895(100)](06)

Юлія САРВАЄВА

Харківський національний університет внутрішніх справ

ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ У КІБЕРПРОСТОРИ

Сьогодні суспільство залежить від соціальних мереж, проводить більшу частину свого часу в Інтернеті. В результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використання мережі Інтернет та/або інших глобальних мереж передачі даних утворюється інтерактивне інформаційне

середовище. Науковці називають таке середовище кіберпростором, або віртуальним середовищем.

Слід розуміти, що користувачі Інтернету – це не лише законослухняні громадяни.

За допомогою комунікаційних систем та/або інших глобальних мереж передачі даних особи із злочинними намірами можуть порушувати авторські права, пропагувати насильство, чинити шахрайство в Інтернеті, розповсюджувати порнографію, продавати наркотичні та психотропні речовини тощо. Організовані злочинні угруповання підтримують зв'язок через інтернет.

Таким чином, у сучасних умовах кіберпростір все більш стає середовищем, яке характеризується побічними ефектами криміногенного характеру.

В багатьох країнах кіберпростір, який зазвичай містить сліди протиправної діяльності злочинців, безперечно стає об'єктом особливої уваги правоохоронних органів цих країн. Зважаючи на зарубіжний досвід та необхідність посилення боротьби зі злочинністю органам внутрішніх справ України необхідно розробити та запровадити відповідні оперативно-розшукові заходи у кіберпросторі.

У зв'язку з цим слід відокремити саму боротьбу із кіберзлочинами від проведення оперативно-розшукових заходів шляхом використання кіберпростору. Вищезазначені заходи можуть проводитись як у справах про кіберзлочини, так і у справах про злочини, скоєні в реальному світі. З метою отримання раніше незнайомої та прихованої інформації, яка становить оперативний інтерес, правоохоронні органи України починають приділяти все більше уваги кіберпростору. Проведення органами внутрішніх справ оперативно-розшукових заходів зі збору та аналізу розміщеної у кіберпросторі інформації спрямовується на розшук доказів (предметів, обставин), що свідчать про скоєння злочинів та/або їх авторів.

На підставі вивчення передового зарубіжного досвіду можна визначити такі основні напрями діяльності органів внутрішніх справ щодо проведення оперативно-розшукових заходів у кіберпросторі: 1) виявлення осіб, які становлять оперативний інтерес; 2) розшук певних осіб з через встановлення їх фізичного розташування; 3) встановлення таємних зв'язків; 4) розшук викрадених речей та виявлення задіяних осіб; 5) здійснення психічного впливу на учасників злочинних структур під час активної діяльності у форумах та чатах.

У теоретичному плані необхідно визначити чіткий перелік оперативно-розшукових заходів у кіберпросторі, визначити задіяні відомства та особи.

Для проведення оперативно-розшукових заходів у кіберпросторі доречно підібрати також відповідні методи. Вважаємо перспективними наступні методи: аналіз відкритих джерел інформації, соціальна інженерія, отримання та аналіз інформації, яка знаходиться в операторів та провайдерів телекомунікацій і т. ін.

На нашу думку, проведення оперативно-розшукових заходів у кіберпросторі буде більш ефективним за умов комплексного застосування органами внутрішніх справ України сил, засобів, заходів та методів. До того, будь-яке застосування засобів, заходів та методів повинно відбуватися лише за умов чіткого та неухильного дотримання вимог чинного законодавства та виключати будь-які прояви порушення прав людини та громадянина.

Науковий керівник І. Л. Іванова

УДК 351.74:001.895](100)(06)

Дар'я СВИСТУН

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Пандемія COVID-19 прискорила потребу в розробці нових технологічних рішень для задоволення непередбачених потреб, таких як виконання функцій поліцією під час пандемії, із заходами соціального дистанціювання. Можливості, які ці технології принесли поліції в епоху COVID-19, продовжуватимуть розвиватися та залишатимуться актуальними протягом наступних років.

У контексті пандемії в законодавстві, що регулює роботу Національної поліції, є деякі нововведення, які можуть допомогти протистояти пандемії. Співробітники Нацполіції мають залучатися до забезпечення карантинних обмежень – недопущення поширення чуток та фейків, які можуть викликати паніку, стежити за діяльністю торгових точок та транспорту, стежити за дотриманням «маскового режиму» в громадських місцях. При цьому від ризику зараження має бути захищена сама поліція.

У контексті того, що пандемія має глобальний характер – розглянемо основні виклики, які стоять перед правоохоронними органами не лише в Україні, а й у всьому світі.

ЗАДАЧА 1: ПЛАНУВАННЯ ГРАФІКІВ РОБОТИ ПЕРСОНАЛУ ТА БЮДЖЕТУ ДЛЯ НЕЗАПЛАНОВАНИХ СИТУАЦІЙ

Укомплектування персоналом, планування та складання бюджету були проблемою для багатьох правоохоронних органів ще до COVID-19.

Багатьом підрозділам потрібно не тільки шукати шляхи мінімізації можливого зараження, але й планувати ймовірність зараження поліцейського. Деяким із цих поліцейських може знадобитися самоізолюватися або взяти відгул по хворобі. Реальність того, що вірус може мати серйозні і навіть смертельні наслідки, означає, що підрозділи також повинні планувати довгострокову втрату працездатності або смерть (а також витрати та кадрові наслідки цих можливостей).

ЗАДАЧА 2: У СИТУАЦІЙНУ ОБІЗНАНІСТЬ ТЕПЕР ВХОДИТЬ ОЦІНКА РИЗИКІВ COVID-19 ДЛЯ ГРОМАДЯН

Оскільки особи, які надають першу допомогу, за самою природою своєї роботи зобов'язані бути серед багатьох людей, іншою проблемою стає те, як забезпечити їх під час пандемії.

Функція миттєвого чату є ефективним інструментом для спілкування в режимі реального часу з хворими пацієнтами або пацієнтами в масках, а також глухими та слабочуючими. А служби визначення місцезнаходження засновані на місцезнаходження пристрою абонента, що дозволяє респондентам точно визначити місцезнаходження навіть у межах будівельного комплексу або густонаселеного району.

ЗАВДАННЯ 3: КОНТРОЛЬ ВІРУСУ ТА ЗАДОВОЛЕННЯ ПОТРЕБ У ГРУПОВОМУ СЕРЕДОВИЩІ ЧЕРЕЗ ЗБІР ДАНИХ

Через спільне середовище та тісні приміщення виправні установи та місця ув'язнення можуть стати гарячими ліжками для випадків COVID-19. За даними Центру з контролю за захворюваннями, оперативне виявлення людей з COVID-19 та послідовне застосування заходів профілактики у виправних установах та місцях ув'язнення мають вирішальне значення для захисту ув'язнених чи затриманих осіб, співробітників та громад, куди вони повертаються.

Juvare створив панель керування пандемією, яка полегшує виправним установам щоденне відстеження випадків, щоб зрозуміти вплив на установи, ув'язнених та персонал.

ЗАДАЧА 4: УПРАВЛІННЯ ПРОБАЦІЄЮ ТА УМОВНО-ДОМОВОЛЬНИМ ЗВІЛЬНЕННЯМ, МІНІМІЗУЮЧИ ОСОБИСТИЙ КОНТАКТ

Ув'язнені, які повертаються до громади, і ті, хто перебуває на випробувальному терміні, вже ризикують знову потрапити в ситуації, що призвели до неприємностей. Одна пропущена реєстрація через транспортування чи інші проблеми може призвести до жаклих наслідків. Пандемія COVID та пов'язані з нею збої роблять проблему ще більшою і змусили агенції по-іншому поглянути на те, як вони використовують технології для управління групою правопорушників.

ЗАДАЧА 5: ЗМЕНШЕННЯ ПОТРЕБИ ЗУСТРІЧІ ОБЛИЧЧЯ-НА-ОБЛИЧЧЯ

Поліцейські відділи вже переповнені, а пандемія COVID-19 потенційно ще більше зменшила ряди. Щоб зменшити ймовірність розкриття, правоохоронні органи повинні визначити пріоритетність типів викликів, які призведуть до відправлення офіцера на місце події.

Оскільки громадяни все частіше використовують такі програми, як FaceTime і Google Hangouts, для взаємодії один з одним у відеочаті. Багато правоохоронців вже використовували телефон МІЖНАРОДНОЇ ГАРЯЧОЇ ЛІНІЇ 10-21, щоб спілкуватися з громадянами по телефону, не повідомляючи їх особистий номер телефону. Коли вдарив COVID, багато з цих офіцерів виявили, що додаток також допоміг їм зменшити потребу в особистих зустрічах для рутинної роботи поліції, яку можна було б виконувати по телефону.

Хоча ці технології були створені або вдосконалені, щоб допомогти правоохоронним органам адаптуватися до умов, що змінюються через пандемію COVID-19, багато з цих проблем існували до пандемії і продовжуватимуть існувати, коли світ пристосовується до нової норми.

Такі переваги, як покращена обізнаність про ситуацію, покращена точність визначення місцезнаходження, більший доступ до даних і спільний доступ до них, а також спрощені процеси призведуть до більшої безпеки для співробітників правоохоронних органів і людей, яким вони обслуговують. Рішення, народжені цією кризою, можуть продовжувати вдосконалюватися, але, безсумнівно, вони тут, щоб залишитися.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Андрій СЕМЧУК

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ПРОГРАМ ДЛЯ АНАЛІЗУ МЕРЕЖЕВИХ ПРОТОКОЛІВ

В епоху високих інформаційних технологій, коли все розвивається стрімкими темпами, злочинці все частіше використовують Інтернет для здійснення своїх злочинів. Проте правоохоронні органи не стоять на місці і використовують більш досконалі методи оперативно-розшукової діяльності. Різновидом цих методів є використання програмних засобів для сканування та аналізу трафіку для комп'ютерних мереж. Ці методи активно використовуються в підрозділах кіберполіції різних Європейських країн.

Одним з таких методів є Wireshark. Wireshark — це програма з відкритим вихідним кодом для аналізу мережевих протоколів, започаткована Джеральдом Комбсом у 1998 році. Глобальна організація мережевих спеціалістів і розробників програмного забезпечення підтримує Wireshark. Wireshark абсолютно безпечний у використанні. Немає кращого способу навчитися працювати в мережі, ніж подивитися на трафік під мікроскопом Wireshark.

Є питання щодо законності Wireshark, оскільки це потужний перебірник пакетів, оскільки слід використовувати Wireshark лише в мережах, де є дозвіл на перевірку мережевих пакетів.

Сучасна бездротова мережева технологія дозволяє особам, які мають сумісну бездротову карту, захоплювати пакети даних, призначені для іншого комп'ютера, завдяки тому, що радіохвилі є носієм, через який передаються дані, надіслані бездротовим способом. Таким чином, поліцейський теоретично може спробувати зібрати цифрові докази проти підозрюваного, знаходячись в безпосередній близькості від підозрюваного та використовуючи карту бездротової мережі свого комп'ютера для захоплення будь-яких пакетів у цьому районі, а потім аналізуючи пакети, щоб спробувати зібрати інформацію, яка може бути корисною для розслідування.

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Яна СКРИПНИК

Харківський національний університет внутрішніх справ

РОЗПІЗНАВАННЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА З МЕТОЮ ІДЕНТИФІКАЦІЇ ЛЮДЕЙ

Важливою є увага до наукових знань та використання різноманітних інноваційних програм у роботі судової влади. Можливість використання різноманітних нових технологій — основа успішної роботи поліції.

Розпізнавання райдужної оболонки ока — це метод біометричних даних з метою аутентифікації або ідентифікації людей. Для цього знімки райдужної оболонки ока робляться спеціальними камерами, визначаються та зберігаються характерні ознаки відповідної райдужної оболонки або порівнюються з одним чи кількома вже збереженими шаблонами. У порівнянні з іншими біометричними системами, такими як розпізнавання обличчя, відбиток пальців, голос, аналіз ДНК, розпізнавання райдужної оболонки ока вважається одним з найнадійніших методів.

Сьогодні в поліції доступні різні системи розпізнавання райдужної оболонки ока людини. Програмне забезпечення для розпізнавання райдужної оболонки ока від DERMALOG забезпечує необхідну якість і точність для захоплення та керування великою кількістю зображень райдужної оболонки ока. Зібрані дані використовуються для реєстрації або перевірки особи.

Наприклад, система розпізнавання райдужної оболонки ока людини, що рухається, яка може визначити особу людини за її райдужною оболонкою з відстані близько 5 метрів. Пристрій дозволяє розпізнати людину без додаткових процедур або зусиль самої людини, тобто людині не потрібно підходити і дивитися в сканер.

Усі ці властивості зробили розпізнавання райдужної оболонки привабливою технологією для використання в системах безпеки. Багато систем розпізнавання райдужної оболонки ока поєднуються з іншими біометричними системами ідентифікації або іншими методами підтвердження ідентифікації для підвищення безпеки. Шанси обійти комбіновану систему ідентифікації відбитків пальців і райдужної оболонки ока дуже невеликі. Інші системи повністю покладаються на системи розпізнавання райдужної оболонки ока, оскільки вони мають дуже маленький потенціал для помилкової ідентифікації. Це нововведення може бути корисним у спеціальних зонах безпеки, таких як перетин кордону. Він також підходить для використання в інших місцях, коли особу потрібно визначити в більшій натовпі.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Карина СТАРЧЕНКО

Харківський національний університет внутрішніх справ

ЧИ ЗАМІНЯТЬ РОБОТИ ПОЛІЦІАНТІВ?

Роботи-поліціянти створені, щоб надати доступ до недоступних або небезпечних місць для швидкого реагування на ситуації. Вони можуть керувати предметами, а також збирати дані за допомогою різноманітних технологій. Такі роботи можуть застосовуватися в різних середовищах із різними можливостями передачі даних і зв'язку. Нові роботи для забезпечення безпеки виконують типову функцію людини: поліціанта під час патрулювання. Вони патрулюють район і реагують на скоєння злочину.

Застосування роботів у поліційній діяльності зараз і на найближчий час включає: постійне розширення можливостей роботів збирати

інформацію про спостереження, приймати звіти поліціантів та забезпечувати комунікацію в умовах, небезпечних для людей.

Компанія передових технологій безпеки Knightscore, що базується в Кремнієвій долині (Сполучені Штати Америки), створює повністю автономних роботів безпеки, які затримують, виявляють і повідомляють. Компанія продала понад 50 своїх автономних роботів безпеки, які працюють на штучному інтелекті, більш ніж 20 клієнтам. Їх конічні п'ятифутові роботи мають чотири камери, що можуть сканувати номерні знаки та розпізнавати MAC-адреси окремих мобільних телефонів. Хоча роботи не схожі на класичного поліціанта в формі синього кольору, вони патрулюють зі швидкістю ходьби, щоб забезпечити безпеку району.

Їхню ефективність до цього часу було важко довести, але за поведінкою вони нагадують гуманоїдних роботів.

Роботи зі штучним інтелектом стають все більш поширеним інструментом для боротьби поліції та інших правоохоронних органів у всьому світі зі злочинністю, але найближчим часом, напевно, роботи не замінять людей, тому що ця робота займає 167 місце з 702, а вищий рейтинг (тобто менший номер) означає меншу ймовірність заміни.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Микита ТАЛАН

Харківський національний університет внутрішніх справ

РОЗВІДКА З ВІДКРИТИХ ДЖЕРЕЛ

Розвідка з відкритим кодом (OSINT) — це збір та аналіз даних, зібраних з відкритих джерел (відкритих і загальнодоступних джерел), для створення практичних розвідувальних даних. OSINT в основному використовується у функціях національної безпеки, правоохоронних органів та бізнес-розвідки і є цінним для аналітиків, які використовують неконфіденційні дані для відповідей на секретні, несекретні чи власні вимоги до розвідки в попередніх дисциплінах розвідки.

Джерела OSINT можна розділити на шість різних категорій потоку інформації:

ЗМІ, друковані газети, журнали, радіо та телебачення з різних країн і між ними.

Інтернет, онлайн-видання, блоги, дискусійні групи, громадянські ЗМІ (тобто – відео для мобільних телефонів і створений користувачами контент), YouTube та інші веб-сайти соціальних мереж (тобто –

Facebook, Twitter, Instagram тощо). Це джерело також випереджає низку інших джерел завдяки своєчасності та простоті доступу.

Публічні державні дані, звіти державного управління, бюджети, слухання, телефонні довідники, прес-конференції, веб-сайти та виступи. Хоча це джерело походить з офіційного джерела, воно є загальнодоступним і може використовуватися відкрито та вільно.

Професійні та наукові публікації, інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дисертацій та дисертацій.

Комерційні дані, комерційні зображення, фінансові та промислові оцінки та бази даних.

Сіра література, технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.

OSINT відрізняється від дослідження тим, що він застосовує процес інтелекту для створення індивідуальних знань, що підтримують конкретне рішення конкретної особи або групи.

OSINT визначається як директором національної розвідки США, так і Міністерством оборони США (DoD), як розвідувальна інформація, «виготовлена з загальнодоступної інформації, яка збирається, експлуатується та своєчасно поширюється серед відповідної аудиторії з метою опрацювання конкретна вимога до розвідки». Згідно з визначенням НАТО, OSINT — це розвідувальна інформація, «отримана на основі загальнодоступної інформації, а також іншої несекретної інформації, яка має обмежене публічне поширення або доступ.

Open Source Intelligence (OSINT) — це інформація, що стосується безпеки, зібрана з вільно доступних відкритих джерел (наприклад, соціальних і професійних мереж, новин, веб-сайтів). Для отримання корисної інформації з різних частин інформації використовуються відповідні аналізу інструменти.

Ці джерела можуть бути безкоштовними або на основі підписки, онлайн або офлайн.

Open Source Intelligence не обмежується Інтернетом, але також може використовувати вільно доступні засоби масової інформації як джерело, такі як журнали, щоденні газети, радіо та телебачення.

OSINT можна використовувати в області кібербезпеки, наприклад, для злову, соціальної інженерії, тестування на проникнення та аналізу безпеки. З цієї причини організаціям має сенс збирати та оцінювати інформацію OSINT і відповідним чином реагувати.

Потенційними джерелами є: форуми та блоги, соціальні та професійні мережі, бази даних з програмними помилками (Vulnerability Data Bases), Deep and Dark Web, оголошення про роботу, веб-сторінки, інші джерела Інтернету.

Переваги інтелекту з відкритим вихідним кодом. Витрати на отримання інформації низькі через зростання ступеня оцифрування та великої кількості вільно доступної інформації в Інтернеті.

Закупівля інформації може бути легко реалізована за допомогою автоматизованих інструментів аналізу.

Ризик виявлення низький, оскільки доступ до інформації здійснюється через публічну інфраструктуру та технології.

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Яна ТЕЛУХА

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В РОБОТІ ПОЛІЦІЇ

Розвиток технологій важко передбачити. Інформація про потенційно актуальні технології, отримана якомога раніше, дозволяє активно використовувати пов'язані з ними можливості для інноваційних оперативних методів та методів розслідування. Розробка нових методів виявлення вибухових речовин, наркотиків, зброї та інших речовин, що мають значення для кримінального переслідування, а також систематичне випробування наявних технологій виявлення належать до основних завдань у цій галузі. Нові технічні розробки активно впроваджуються у виконання поліцейських завдань.

Індивідуальні біологічні ознаки (відбитки пальців, голос, обличчя, очі тощо) також будуть використовуватися для ідентифікації особи в найближчому майбутньому. Але сьогодні відбитки пальців більше не зрівнюються вручну, а за допомогою автоматичних систем ідентифікації відбитків пальців.

Сучасні технології, тактики та нові способи збору, фіксування та передачі інформації вже давно увійшли в повсякденне життя поліції. Збільшення обсягу цифрових даних створює виклик для органів безпеки. Цьому процесу слід протидіяти сучасними методами інтелектуального аналізу. Звичайне програмне забезпечення не завжди можна використовувати для потреб поліції. Тому часто розробляються спеціальні програмні забезпечення та методи.

Нові інформаційно-комунікаційні технології змінили рівень та інтенсивність поліцейського контролю. До них відносяться нові версії відеоспостереження: вони не лише дають змогу відстежувати переміщення людини на екрані по цілих будівельних комплексах або навіть у центрі міста. Вони використовують синергію інших нових

технологій, наприклад, біометричних процесів, та автоматизують контроль транспортних засобів або людей.

Зростаюче проникнення сучасних технологій та засобів комунікації в усі сфери життя відкриває немислені досі можливості для вчинення кримінальних правопорушень. Федеральне управління кримінальної поліції уважно спостерігає за прогресом в цій галузі і розробляє власні стратегії та методи як для профілактики злочинів так і кримінального переслідування.

Науковий керівник Г. М. Сорокіна

УДК 351.74:001.895](100)(06)

Олександр ТЕСЛЕНКО

Харківський національний університет внутрішніх справ

ФІШИНГОВА АТАКА ЯК ВИД КІБЕРЗЛОЧИНУ

Фішинг – це коли зловмисники надсилають шахрайські електронні листи, прикидаючись від законних компаній, намагаючись зібрати конфіденційну особисту інформацію. Часто будь-які посилання в електронному листі переспрямовують на веб-сайт, що належить шахраю, тому завжди будьте обережні з інформацією, яку ви надаєте в Інтернеті.

Фішинг – це тип атаки соціальної інженерії, яка часто використовується для крадіжки даних користувачів, зокрема облікових даних для входу та номерів кредитних карток. Це відбувається, коли зловмисник, маскуючись під довірену особу, обманює жертву, щоб вона відкрила електронний лист, миттєве повідомлення або текстове повідомлення. Потім одержувача обманом заставляють натиснути шкідливе посилання, що може призвести до встановлення зловмисного програмного забезпечення, зависання системи в рамках атаки програм-вимагачів або розкриття конфіденційної інформації. Атака може мати руйнівні наслідки. Для фізичних осіб це включає несанкціоновані покупки, крадіжку коштів або крадіжку особи. Крім того, фішинг часто використовується, щоб закріпитися в корпоративних або урядових мережах як частина більш масштабної атаки, наприклад, подія розширеної стійкої загрози (APT). У цьому останньому сценарії співробітники скомпрометовані, щоб обійти периметри безпеки, поширити шкідливе програмне забезпечення в закритому середовищі або отримати привілейований доступ до захищених даних. Організація, яка піддається такій атаці, зазвичай несе серйозні фінансові втрати на додаток до зниження частки ринку, репутації та довіри споживачів.

Залежно від масштабу спроба фішингу може перерости в інцидент безпеки, після якого компанії буде важко відновитися.

Фішинг електронної пошти - це гра чисел. Зловмисник, який розсилає тисячі шахрайських повідомлень, може отримати значну інформацію та суми грошей, навіть якщо лише невеликий відсоток одержувачів потрапляє на шахрайство. Як було показано вище, зловмисники використовують деякі прийоми, щоб підвищити рівень успіху. По-перше, вони докладуть чимало зусиль, створюючи фішингові повідомлення, щоб імітувати фактичні листи від підробленої організації. Використання однакових фраз, шрифтів, логотипів і підписів робить повідомлення легітимними. Крім того, зловмисники зазвичай намагаються підштовхнути користувачів до дії, створюючи відчуття невідкладності. Наприклад, як було показано раніше, електронний лист може загрожувати закінченням терміну дії облікового запису та поставити одержувача на таймер. Застосування такого тиску призводить до того, що користувач стає менш старанним і більш схильним до помилок.

Як запобігти фішингу? Захист від фішингових атак вимагає вжиття заходів як користувачами, так і підприємствами. Для користувачів важлива пильність. Підроблене повідомлення часто містить незначні помилки, які розкривають його справжню ідентичність. Вони можуть включати орфографічні помилки або зміни доменних імен. Користувачі також повинні зупинитися і подумати, чому вони взагалі отримують такий електронний лист.

*Консультант з мови **В. В. Кочина***

УДК 351.74:001.895](100)(06)

Ілона ТИМОФІЄНКО

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Важливу роль у діяльності правоохоронних органах, відіграє злочинність. Боротьба зі злочинністю ведеться в усіх країнах, різними державними організаціями, підприємствами, громадянами. Запобігати злочинам потрібно на початковому етапі, коли злочинець тільки замишляє та планує вчинення певного діяння.

На сьогоднішній день, ефективність діяльності правоохоронних органів, залежить від технічного оснащення. Якщо бути точнішим, в практичну діяльність органів Національної поліції України, широко впроваджується злічувальна техніка, автоматизовані робочі місця, які

обладнані сучасними персональними комп'ютерами та великою базою даних. Це допомагає практичним працівникам, вони менше виконують одноманітну роботу, тобто вся праця покладена на технічне оснащення. Сьогодні, технології допомагають знаходити рішення при розв'язанні різноманітних питань, дають можливість ширше вивчати процеси, розібрати їх.

В умовах зростаючої комп'ютеризації, у тому числі і в Національній поліції України, головною метою процесу розвитку, є надання курсантам, студентам та слухачам закладів вищої освіти МВС України, працівникам органів Національної поліції спеціальних знань, умінь та навичок з іноваційних технологій та інформаційного забезпечення їх професійної діяльності, які ефективно використовують комп'ютерну техніку та сучасні інформаційні технології у своїй оперативно-службовій діяльності.

Функція миттєвого чату є важливим інструментом для спілкування в режимі реального часу з хворими пацієнтами або пацієнтами в масках, а також глухими. А служби визначення місцезнаходження засновані на місцезнаходження пристрою абонента, що дозволяє точно визначити, де перебуває особа. Незважаючи на те, що для стеження за людьми необхідно мати спеціальний дозвіл від відповідних установ, існує не менше трьох способів, як можна дізнатися місце розташування людини за його номером телефону. Це буває необхідно, коли потрібно знайти дитину, що загубилась або злочинця, що в пошуку. Пошук людей за номером телефону можливий через спеціалізовані програми. Ці знання потрібно покращувати і розвивати через інформаційні технології.

Коли вдарив COVID, багато офіцерів зрозуміли, що функції миттєвого чату також допомагають їм зменшити потребу в особистих зустрічах для рутинної роботи поліції, яку можна було б виконувати по телефону.

Хоча ці технології були створені або вдосконалені, щоб допомогти правоохоронним органам адаптуватися до умов, що змінюються через пандемію COVID-19, багато з цих проблем існували до пандемії і продовжуватимуть існувати, коли світ пристосовується до нової норми.

Спрощені процеси призведуть до більшої безпеки для співробітників правоохоронних органів і людей, яких вони обслуговують, потрібно покращити обізнаність у сфері іноваційних технологій, тоді покращиться точність визначення місцезнаходження, швидше почнуть розвиватись функції миттєвого чату, більше автоматизувати робочі місця, які обладнані сучасними персональними комп'ютерами та великою базою даних, тоді зросте довіра населення до правоохоронних органів, а це головне.

Мовний консультант А. В. Білоусов

УДК 351.74:001.895](100)(06)

Ельвіра ТКАЧЕНКО

Харківський національний університет внутрішніх справ

НОВІТНІ ТЕХНОЛОГІЇ ДОПОМАГАЮТЬ ПОЛІЦІЇ БОРОТИСЯ ЗІ ЗЛОЧИННІСТЮ

Поліційні машини пройшли довгий шлях з того часу, як перший поліційний автомобіль виїхав на вулиці Акрона, штат Огайо, у 1899 році (з сиреною та камерою для ув'язнених в задній частині машини).

Інновації в сучасних поліційних машинах (і тих, які будуть у майбутньому) привели до таких оновлень, як використання клавіатури ноутбука, планшетів і вбудованих комп'ютерів, підключених до Wi-Fi, що надає поліціянтам перевагу мати миттєвий доступ до важливої інформації, систем зв'язку тощо.

Розширені можливості відеореєстратора дуже корисні для спостереження та збору інформації, а також для доказування та підзвітності. Функції безпеки поліціянта в машинах наступного покоління (наприклад, бронебійні куленепробивні двері) також впроваджуються в деякі поліційні машини, а можливості напівавтономної технології вже у недалекому майбутньому.

Та ж сама технологія, яка дає можливість збирати мито за проїзд, автоматично сканує та заносить у базу даних реєстраційні номери та літери номерного знаку, щоб стягнути плату, зараз використовується поліцією для різних цілей, від виявлення викрадених автомобілів до наздоганяння людей, які мають активні ордери або моніторинг «Amber Alerts». Однак технології, які правоохоронні органи використовують для автоматичного розпізнавання автомобільних номерів (ALPR), зробили ще один інноваційний крок уперед.

Новітня технологія ALPR поєднує офіційну технологію ідентифікації з ШІ (штучним інтелектом), що надає правоохоронним органам право надійно та послідовно ідентифікувати номерні знаки.

За допомогою штучного інтелекту камери ALPR можуть ідентифікувати марку, модель та колір автомобілів навіть при слабкому освітленні та поганій погоді, розрізняти окремі символи на номерних знаках, виявляти нові номерні знаки в міру їх появи та розширювати базу даних оновленими та незнайомими зразками.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Юлія ТУЯХОВА

Харківський національний університет внутрішніх справ

ПЕРЕШКОДИ В ОРГАНІЗАЦІЙНИХ КОМУНІКАЦІЯХ

Перешкоди, що виникають у сфері комунікацій, поділяють на перешкоди в комунікаціях між особами та в організаційних комунікаціях.

До бар'єрів на шляху міжособових комунікацій відносять:

- перешкоди, що зумовлені сприйняттям;
- семантичні бар'єри;
- невербальні перешкоди;
- поганий зворотній зв'язок;
- невміння слухати.

Перешкодами в організаційних комунікаціях є:

- викривлення повідомлень;
- інформаційні перевантаження;
- незадовільна структура організації.

В статті буде розглянуто перешкоди в організаційних комунікаціях в поліцейській сфері.

Першим пунктом може бути-викривлення повідомлень, це коли інформація рухається всередині організації вгору й вниз, зміст повідомлень дещо змінюється. Таке змінення може бути зумовлено зовсім різними причинами. Повідомлення можуть викривлятися випадково через труднощі в контактах між особами . Коли керівник не згоден з інформацією, повідомленням може вийти свідоме викривлення інформації . У такому разі він модифікує повідомлення таким чином, щоб зміна змісту відбувалася в його інтересах.

Через викривлення повідомлень можуть вийти проблеми обміну інформації також можуть бути унаслідок фільтрації. У кожній організації фільтрують інформацію, яку вони отримують, для того щоб правильне повідомлення відправити до правильного відділу організації або на інший рівень.

Для того щоб прискорити рух інформації в організації різноманітні відомості спрощуються перед направленням у різні сегменти організації.

Через різні статуси рівнів організації, повідомлення , що надходять "вгору" чи "вниз" можуть бути викривленими.

Часто чим вище статус рівня організації , внаслідок набуває тенденція надавати їм лише позитивну інформацію. Після цього, як правило, відбувається те, що співробітник (підлеглий) не інформує свого прямого начальника про якусь проблему, або потенціальну проблему, оскільки це вже для нього "не бажана (не позитивна) інформація".

Наступним чином відбуваються інші події, підлеглі далі повідомляють свого начальника лише про ту інформацію за яку б вони отримали схвалення, або те що він хоче почути.

Це вважається найпоширенішою причиною викривлення інформації.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Аріна УСЕНКО

Харківський національний університет внутрішніх справ

АВТОМАТИЧНІ ПРИСТРОЇ НА СЛУЖБІ ПОЛІЦІЇ

Автоматизація – це широке поняття, яке описує всі процеси, які виконуються автоматично за допомогою програмного забезпечення або роботів. Тобто це завдання, які виконуються без участі людини. Роботизація охоплює лише ту частину цієї практики, коли на зміну людям приходять автоматичні механізми.

Поява керованих державою автономних поліцейських роботів не виглядає як передбачення в науково-фантастичних фільмах. Армія роботів зі зброєю не вибиває двері з метою накладання арешту. Поліцейські роботи, можливо, не зможуть завдати шкоди людям, як озброєні дрони-хижакі, які використовуються в бою, але, як показує історія, виклик поліції може виявитися не менш смертельним.

Поліцейські роботи створені для надання доступу до ситуацій, які є недоступними або небезпечними для швидкого реагування, і можуть маніпулювати об'єктами, а також збирати дані за допомогою різноманітних технологій. Ситуації вимагають застосування роботів, придатних для різноманітних середовищ з різними можливостями передачі даних і зв'язку.

Так наприклад, роботам Knightscope потрібні камери для навігації та проходження місцевості. Ці роботи оснащені багатьма інфрачервоними камерами, здатними зчитувати номерні знаки. Вони також мають бездротову технологію, здатну ідентифікувати смартфони в межах свого діапазону до MAC та IP.

Поліція приділяє багато уваги тестуванню «собак-роботів», яких вона використовувала в кількох ситуаціях, в тому числі для доставки їжі в ситуації з заручниками та для розвідки місця, коли поліція побоювалася, що може ховатися небезпечний стрілець.

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Ілля УСТИМЕНКО

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

У ХХІ столітті з'явилися нові інструменти та категорії в боротьбі зі злочинністю. Технології змінюються, і все більше департаментів поліції використовують дрони як очі в небі. У 2016 році ці технології тільки впроваджувалися в відомствах, а тепер, зі швидкими темпами технологічного розвитку, підрозділи знаходять нові інноваційні способи використання цих пристроїв для підвищення громадської безпеки, затримання злочинців та порятунку життя.

Дрони, нагрудні відеореєстратори, програмне забезпечення для розпізнавання обличчя, штучний інтелект та багато інших є найважливішими технологіями, які забезпечують правоохоронні органи новими можливостями для захисту та несення служби.

Програмне забезпечення для розпізнавання обличчя є однією з найбільш суперечливих технологій, що з'явилися в поліції. Коли ця система вперше потрапила до правоохоронних органів, багато людей були стурбовані тим, що її використання неетичне. На щастя, це не так, і система розпізнавання обличчя виявляється ефективним інструментом розслідування.

Метою програмного забезпечення для розпізнавання обличчя є те, що в декількох випадках воно допоможе підвищити безпеку. За допомогою програмного забезпечення для розпізнавання обличчя поліціянти Нью-Йорка змогли знайти та затримати підозрюваного у згвалтуванні протягом 24 годин. Оскільки система розпізнавання обличчя дуже перспективна, Міністерство внутрішньої безпеки США стверджує, що до 2023 року її будуть використовувати серед 97% подорожуючих.

Поліція вже більше століття використовує відбитки пальців для ідентифікації людей. Тепер, окрім розпізнавання обличчя та ДНК, правоохоронні органи постійно використовують комплексні дані біометричних (і поведінкових) характеристик. До них відноситься розпізнавання голосу, відбитків долонь, вен зап'ястя, розпізнавання по райдужній оболонці, аналіз ходи та навіть серцебиття.

Науковий керівник Л. С. Сазанова

УДК 351.74:001.895](100)(06)

Дар'я ФАРТУШНА

Харківський національний університет внутрішніх справ

НОВІ ТА ВДОСКОНАЛЕНІ ГАДЖЕТИ ДОПОМАГАЮТЬ ПОЛІЦІЇ МІННЕАПОЛІСА ЗАПОБІГАТИ ЗЛОЧИНАМ

Робота поліціанта раніше вважалася пов'язаною зі звичайними перевітками транспортних засобів та купую робочих документів. Але сьогодні все змінилося. Технологічні зміни в правоохоронних органах накладають свій відбиток на поліцейні відділи по всій країні, оскільки нові та вдосконалені гаджети стають доступними, щоб допомогти поліціантам запобігти злочинам. Є найкращі гаджети, які працівники правоохоронних органів можуть використовувати, щоб виконувати свою роботу та зробити свій район безпечнішим. Роботи-камери з дистанційним управлінням (роботизовані камери) є одним з технічних засобів в арсеналі відділів поліції Міннеаполіса сьогодні.

Поліціанти не можуть бути одночасно на усіх місцях скоєння злочину, а деякі ситуації занадто небезпечні, щоб ризикувати відправленням туди поліціантів. Ось чому роботи були спеціально розроблені для використання в місцях, до яких поліціанти не можуть дістатися безпечно. Коли надто небезпечно відправити поліціанта на місце скоєння злочину, або в будь-якій ситуації, яка вимагає "очей", де немає чіткої картини огляду, поліція може покладатися на роботизовану камеру. Пристрій має електродвигун і спеціальні колеса, які дозволяють йому рухатися, підніматися і проводити дослідження, за бажанням поліціанта, який керує ним дистанційно, що допомагає уберегти поліціанта від небезпеки. Роботизовані камери можна використовувати як у приміщенні, так і на вулиці. У Міннеаполісі поліція використовує їх для виявлення бомб, застосовуючи пульт дистанційного управління, щоб послати їх під транспортні засоби для пошуку підозрілих пакунків.

Завдяки цій роботизованій камері, управління роботом з дистанційним керуванням більше не є дитячою мрією. Поліціанти можуть відправити їх у важкодоступні місця, або місця без чіткої видимості та безпечно керувати ними дистанційно. Поліціанти використовують цю роботизовану технологію не лише для виявлення бомб, але й для обшуку підозрілих будинків і транспортних засобів.

Але є і деякі особливі вимоги, коли справа доходить до експлуатації цього пристрою. По-перше, поліціанти мають бути спеціально підготовлені для керування ним. По-друге, під час використання пристрою на небезпечному місці злочину оператор повинен бути в

супроводі співробітника, щоб прикрити та захистити його, оскільки його увага буде зосереджена на пристрої.

Науковий керівник Олександр Олішевський

УДК 351.74:001.895](100)(06)

Сергій ХАРА

Харківський національний університет внутрішніх справ

РОЗПІЗНАВАННЯ ОБЛИЧ У РЕАЛЬНОМУ ЧАСІ: ДОСВІД ВЕЛИКОЇ БРИТАНІЇ

Технологія розпізнавання облич використовується для ідентифікації осіб або для підтвердження особистості. Наприклад, поліція Південного Уельсу використовує технологію розпізнавання облич для запобігання та виявлення злочинів і захисту вразливої категорії осіб.

Технологія розпізнавання облич аналізує ключові риси обличчя та створює математичне представлення цих рис. Потім ці риси порівнюються з математичним представленням доданих облич у базу даних, генеруючи можливі збіги. Поліція Південного Уельсу використовує розпізнавання облич в реальному часі (LFR). Функція розпізнавання облич у реальному часі (LFR) порівнює зображення обличчя з камери в режимі реального часу із заздалегідь визначеним списком. Дана технологія використовується для визначення місцезнаходження осіб, які становлять інтерес для поліції, шляхом створення сповіщення, коли знаходиться можливий збіг. Перед використанням LFR створюється список правопорушників, яких розшукує поліція та суд. У список спостереження також входять люди, які можуть становити небезпеку для себе чи інших. Після отримання сповіщення про можливий збіг офіцер порівнює зображення з камери з людиною, яку бачить, і вирішує, чи є необхідність розмовляти з нею. Особи, які не включені до списку спостереження, не можуть бути ідентифіковані. Технологія розпізнавання обличчя в реальному часі вважається дієвою та ефективною поліцейською тактикою для запобігання та виявлення злочинів, а також захисту найбільш вразливих верств населення нашого суспільства. Поліція зазвичай використовує цю технологію на громадських заходах і в людних місцях. Поліція Південного Уельсу робить усе можливе, щоб повідомити громадськість про те, де вони використовують технологію розпізнавання обличчя, наприклад: онлайн, перед використанням; за допомогою веб-сайту поліції Південного Уельсу, на якому публікуються результати

використання LFR; за допомогою плакатів та вивісок з QR-кодами, щоб люди знали, що LFR використовується і куди вони можуть звернутися, щоб знайти додаткову інформацію, а співробітники поліції завжди готові пояснити громадськості, як працює LFR і чому вони його використовують.

Існує багато переваг, які розпізнавання облич може дати суспільству, від запобігання злочинам та підвищення безпеки й безпеки до зменшення непотрібної взаємодії з людьми та праці, і очевидно, що українська поліція має й надалі впроваджувати такі технології у свою повсякденну роботу.

Консультант з мови: Н. В. Краснова

УДК 351.74:001.895](100)(06)

Максим ХАРЧЕНКО

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦІЇ

Поліцейські інновації часто згадуються в поліцейській літературі, але вона рідше визначається, застосовується або функціонує вченими. Така ситуація призвела до визначення двозначності і варіації, що обмежує розвиток інновацій як наукової конструкції. Керівники також, здається, класифікують інноваційність з точки зору корисності, яку інновації надають організаційним операціям.

Напевно, багато людей бачили відео, на якому дрони ганяються за порушниками карантину, закликаючи їх повернутися додому. З одного боку, це виглядає смішно, але використання дронів в роботі правоохоронних органів значно полегшує наглядову, слідчу і навіть правоохоронну діяльність поліції. Наприклад, безпілотні літальні апарати (БПЛА) точніше фіксують сцени кримінальних правопорушень, виконують функції рятувальників, стежать за громадськими місцями, збирають дані за допомогою технології GPS, яка потім використовується для кримінологічних і судово-медичних досліджень.

Звичайно, дрони – далеко не єдине «вау-ефективність» нововведення, яке використовується правоохоронними органами для кращого захисту населення та підтримки правопорядку. Але про це варто дізнатися більше.

Дрони. Тему безпілотних літальних апаратів важко вичерпати в декількох вступних пунктах. Їх використання викликає безліч юридичних і безпекових суперечок: від найбільш очевидного порушення недоторканності приватного життя до використання

безпілотників в розвідувальних і військових цілях і порушення повітряних кордонів.

У 2018 році CNN опублікував статтю про використання дронів найбільшим поліцейським департаментом США - департаментом поліції Нью-Йорка. За словами начальника відділу Теренса Монегана, використання БПЛА необхідно в надзвичайних ситуаціях, а тому порушень конфіденційності не очікується. Однак правозахисники та громадяни не підтримують цю думку.

Згідно зі звітом дослідницького центру drone College за березень 2020 року, близько 102 країн використовують БПЛА у військових цілях. У сфері правоохоронних органів дронами користуються близько 1578 державних і муніципальних установ.

Що стосується України, то БПЛА використовується водною поліцією для виявлення порушників карантинного режиму, Консультативна місія ЄС тренує судово-медичні відділи Національної поліції у використанні дронів, а проблему спалювання листя, яка цього року переросла в трагедію, намагалися вирішити у 2018 році за допомогою БПЛА.

Редиктивна поліція

Редиктивна поліція є дуже перспективною практикою використання штучного інтелекту в поліції. Уявіть собі світ, де поліція чекає під будівлею банку правопорушника, перш ніж станеться пограбування. Це звучить як утопія, однак, виходячи з зібраних і оброблених великих даних, така перспектива цілком ймовірна.

Технологія вперше обговорювалася в 2008 році, коли начальник департаменту поліції Лос-Анджелеса Вільям Браттон почав розробляти методи запобігання злочинності за підтримки Бюро допомоги юстиції та Національного інституту юстиції.

Сам метод прогнозування класифікується, однак із загальних джерел можна отримати уявлення про те, які частини даних повинні бути зібрані і оброблені: історія злочинів в певній області (як правило, невелика площа, як і частини міста); збір характеристик попередніх правопорушників; збір даних з систем відеоспостереження; оцінка потенціалу осіб у вчиненні певних видів злочинів; міські оцінки; частота аварій на певній ділянці; матеріального забезпечення мешканців досліджуваної території тощо.

Роботи та самокеровані поліцейські машини

Зазвичай, коли ми чуємо слово «робот», ми уявляємо людиноподібного кіборга, який або хоче захопити світ, або хоче отримати громадянство Дубая. Однак роботи менш гуманні і функціональні. Однак це не заважає їм запобігти вчиненню злочинів або їх суспільно небезпечних наслідків... Іноді досить дивними способами.

Патрульна поліція, вдаючись до поліцейських заходів, зокрема до зупинки транспортних засобів, може зіткнутися з неадекватною, а іноді і небезпечною реакцією з боку водія. У Сполучених Штатах, де носіння зброї є конституційним правом особи, такі випадки не рідкість. Саме тому був винайдений робот-зупинка руху - аналог, який може діяти замість реальної людини і знижувати ризики використання вогнепальної зброї. Функціональна робота включає сканування водійських посвідчень, видачу штрафних квитанцій, затримання водіїв за допомогою «шипової руки».

Також варто згадати про роботів-деактивованих бомб (предком яких є екс-газонокосарка з пультом дистанційного керування Wheelbartow, винайдена в 1972 році), самохідні поліцейські машини (рекомендую прочитати суперечливі погляди на цей рахунок в роботі Ендрю Грегга) і навіть про потенційних заміників людських поліцейських, таких як грабіжники.

Використання роботів в правоохоронних органах - це не просто інноваційне проведення часу. Це можливість для держави заощадити на пенсійних та інших соціальних виплатах, що виплачуються правоохоронцям, можливість захистити поліцейських від професійних травм і врятувати їм життя, і нарешті - підвищити ефективність профілактичних, профілактичних і правоохоронних заходів.

Науковий керівник А. В. Білоусов

УДК 351.74:001.895](100)(06)

Діана ЧАГОВЕЦЬ

Харківський національний університет внутрішніх справ

ТЕХНОЛОГІЧНІ ДОСЛІДЖЕННЯ, ЯКІ ДОПОМАГАЮТЬ РОЗКРИТИ ЗЛОЧИННИ

Досягнення останніх років забезпечили професіоналів правоохоронних органів технологіями, які не тільки полегшують їх роботу, але й водночас забезпечують їх безпеку. Хоча цей список може бути нескінченним, ось деякі з найважливіших технологічних досягнень, які допомогли в боротьбі зі злочинністю.

Відображення даних. Тенденція відображення даних не нова; насправді, метеорологи та кліматологи роблять це протягом десятиліть. Однак фахівці з кримінальної юстиції зараз також збирають дані, надаючи поліцейським департаментам, а також федеральним агентствам чіткий географічний погляд на види злочинів і обсяги злочинів, які відбуваються в певній місцевості. Це корисно для правоохоронних

органів, оскільки показує тенденції, які можна простежити до певних місць; зловживання наркотиками є яскравим прикладом того, як відображення даних може бути корисним для поліції. Це також допомагає поліції визначити проблеми в громаді та дозволяє їм ефективно розробляти стратегію, щоб допомогти зменшити злочинність.

Відстеження смартфона. Хоча існують певні дебати щодо того, коли і як відстеження смартфонів має використовуватися правоохоронними органами, можливість відстежувати злочинця за допомогою його смартфона є неймовірним прогресом у технологіях. Ця технологія при доступі через законні канали може надати правоохоронним органам чітку картину пересування підозрюваного до, під час і після злочину. Для тих, хто невинний у злочині, в якому їх звинувачують, технологія може врятувати їх від кримінального суду; для тих, хто винен, можливість відстеження цього загального об'єкта може закріпити їхню долю.

Соціальні мережі. Соцмережі зробили великий вплив на правоохоронні органи. Багато правоохоронних органів і відділів поліції мають спеціальні акаунти в соціальних мережах на різних платформах, що дозволяє їм взаємодіяти зі своїми спільнотами та діяти за підказками в режимі реального часу. Це стало неоціненним для розкриття злочинів, оскільки дає змогу поліції чи іншим правоохоронним органам отримувати найсвіжішу інформацію про триваючий злочин або нещодавній злочин, просто звертаючи увагу на свої стрічки соціальних мереж. Це також корисно для оцінки того, як громада ставиться до своєї взаємодії з поліцією; тепер зрозуміло, що безпосередня взаємодія з правоохоронними органами зміцнює довіру, дозволяючи жертвам і свідкам надавати інформацію про злочини.

Біометрія. Більшість американців звикли до біометрії; це технологія, яка дозволяє їм розблокувати свої смартфони за допомогою відбитка пальця або сканування райдужної оболонки ока. Ця технологія існує протягом десятиліть, але лише нещодавно вона стала доступною для населення. Сфера кримінальної юстиції тепер скористалася цією технологією і створила менші пристрої для ідентифікації, які дають змогу виявляти злочинців з минулими записами або невиконаними ордерами, не чекаючи на процес, який може зайняти тижні або місяці. Ці портативні пристрої можна використовувати на місці злочину для збору цифрових відбитків пальців, а потім використовувати на свідках, щоб побачити, чи злочинець все ще знаходиться на місці злочину.

Технології продовжують покращувати правоохоронну діяльність і, у свою чергу, відносини між правоохоронцями та громадами, яким вони обслуговують. Забезпечуючи різні способи боротьби зі злочинністю, технологія зробила громади безпечнішими для життя та роботи. З

огляду на все більший розвиток, професіонали, які прагнуть отримати ступінь кримінального судочинства, виявлять, що технології і надалі відіграватимуть велику роль у тому, як кримінальне правосуддя буде виглядати в найближчі роки.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Тимофій ЧАЙКІН

Харківський національний університет внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПОЛІЦІЇ

У США понад 910 організацій, включаючи поліцію та пожежні підрозділи, використовують дрони для збору доказів і відстеження подій на відстані. За словами колишнього заступника комісара поліції Філадельфії Ноли Джойс, правоохоронні органи також використовують системи виявлення вогнепальної зброї, автоматичні зчитувачі номерних знаків і програми розпізнавання облич. Тим часом у США інженер-механік з Каліфорнійського науково-дослідного інституту SRI International розробив робота, щоб допомогти поліцейським уникнути потенційних конфліктів з водіями.

Ще одна система помічників незабаром з'явиться у поліції Великобританії. За його допомогою правоохоронці планують прогнозувати вчинення тяжких злочинів насильницького характеру з використанням технологій штучного інтелекту. Використовується комбінація ШІ (штучний інтелект) і статистика. Для пошуку «майбутніх» злочинців система оцінює понад 1,4 тисячі характеристик. Алгоритми ШІ розраховують людину, яка знаходиться в групі ризику, і дає оцінку ймовірності вчинення ним злочину із застосуванням зброї. Про використання цифрових технологій для підвищення безпеки співробітників і громадян: Інтернет речей і розподілене зондування – це використання нових технологій для збору інформації та визначення правильного напрямку. Але що робити офіцерам на місці події? Розробляються нові технології та методи, які можуть допомогти керувати дії у всьому світі. Досягнення в таких областях, як зв'язок 5G, мініатюризація електроніки та доповнена реальність, дають людям змогу бачити, чути та діяти так, як це було раніше неможливо. Наприклад, офіцер, який прибуває в незнайомій ситуації, тепер може використовувати окуляри доповненої реальності, щоб побачити відповідну інформацію про попередні виклики служби з цієї адреси, знайти виходи з будівлі або переглянути недавню історію злочинів

блоку. Маючи цю інформацію, офіцер може вжити запобіжних заходів, щоб захищати себе та служити громаді.

Науковий керівник Л. І. Русанова

УДК 351.74:001.895](100)(06)

Дар'я ЧАЙКОВСЬКА

Харківський національний університет внутрішніх справ

НЕПЕРЕДБАЧУВАНІ НАСЛІДКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ У ПОЛІЦЕЙСЬКІЙ РОБОТІ: ДОСВІД ДОКТОРА ДЖАРРОДА САДУЛЬСЬКІ

Доктор Джаррод Садульскі є ад'юнкт-професором Американського військового університету. Більше двох років він вивчав поліцейський стрес та його вплив на життя поліцейських. Він каже: «Хоча технології, безсумнівно, були корисними для поліції, багато з цих досягнень також мали несприятливий — і часто нехтували — вплив на роботу поліції».

Технологічний прогрес спричинив серйозні зміни в поліцейській діяльності за останні кілька десятиліть. Порівняно з минулими поколіннями, сьогодні офіцери оточені технологіями, які мають на меті підвищити продуктивність, безпеку офіцерів та ефективність роботи агентства. Спілкування, наприклад, було значно покращено. Часи зв'язку з диспетчерськими лише через традиційне поліцейське радіо або відстеження таксофону, щоб подзвонити на станцію, давно минули. Сьогодні офіцери мають мобільні телефони і несуть відповідальність за моніторинг зв'язку через передові поліцейські радіоприймачі, які можуть сканувати багато каналів або районів одночасно. Поліцейські машини також оснащені передовими комп'ютерними системами диспетчеризації. Ці системи диспетчеризації покращують швидкість реагування офіцерів на виклики, допомагають у зборі слідчих даних та очищають дзвінки без радіозв'язку. Було також багато інших досягнень. Наприклад, у понад 7 000 поліцейських відомств було розгорнуто прилади кондуктивної енергії, такі як електрошокери. Дослідження показують, що ці пристрої сприяли зниженню травм офіцерів на 25-62 відсотки (MacDonald, Kaminski, & Smith, Michael 2009). Інші технології також допомогли офіцерам бути більш ефективними та ефективними. Наприклад, камери світлофора дозволили патрульним зосередитися на проблемних ділянках і допомагали їм у дотриманні правил дорожнього руху.

Навчання та застосування багатьох із цих передових технологій пов'язані з значним стресом. Очікується, що офіцери опанують

технології і, на жаль, не завжди отримують належну підготовку, необхідну для того, щоб використовувати їх на рівні майстерності. Багато офіцерів відчують, що їм нав'язують різні технології, створюючи некеровану кількість речей, які потрібно навчитися і запам'ятати. Керівникам агенцій важливо усвідомити, що адаптація нових технологій часто викликає стрес для офіцерів, тому їм потрібно вжити заходів, щоб допомогти полегшити частину цього стресу. Технологія може мати непередбачувані наслідки, коли офіцери повинні звертати увагу на таку кількість різних пристроїв. Наприклад, хоча кожна з комп'ютерних систем диспетчеризації, стільникових телефонів та інших комунікаційних пристроїв має свої переваги, вони можуть бути надзвичайно відволікаючими для офіцерів і навіть небезпечними, коли їхня повна увага потрібна для однієї ситуації. Наприклад, коли офіцер керує патрульним підрозділом, дзвінки в службу зазвичай надсилаються на ноутбук офіцера в автомобілі через комп'ютерну диспетчерську систему. Посилання на цю технологію під час водіння підвищує ризик ДТП для офіцерів. Постійне розподілення уваги між різними пристроями може призвести до потенційно небезпечної ситуації та викликати у офіцерів постійний стрес. Іншим джерелом стресу для офіцерів є те, що деякі з цих технологічних досягнень не спрацюють, коли їм це потрібно. Тепер офіцери оснащені менш смертельною передовою зброєю, як-от електрошокери, та боекприпасами, які включають перцеві патрони та гумові снаряди. Якщо ці пристрої не працюють належним чином, офіцери можуть постраждати.

У той час, коли управління стресом у поліції має вирішальне значення для підвищення стійкості та міцного здоров'я офіцерів, можна вжити заходів для зменшення стресу, пов'язаного з технологіями. Приклади включають: впровадження адміністративної політики або особистих цілей, спрямованих на зменшення відволікань; встановити стандарт спілкування з диспетчером та керівниками під час виконання службових обов'язків; дозволяти офіцерам використовувати технологію, яка їм зручна, коли це можливо; Надайте належний час для навчання офіцерів новим технологіям.

Підсумовуючи, технологія принесла багато переваг для правоохоронних органів. Сучасне технологічне обладнання може зменшити нестачу робочої сили, підвищити безпеку офіцерів і допомогти офіцерам виконувати свою роботу легше. Проте технології також можуть стати стресом для офіцерів. Важливо, щоб агенції визнали цей стрес і вжили заходів, щоб допомогти офіцерам стати досвідченими та зручними у використанні технологій

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Руслан ЧУБЕНКО

Харківський національний університет внутрішніх справ

ЗАЛУЧЕННЯ РОБОТІВ ВІД КОМПАНІЇ «BOSTON DYNAMICS» ДЛЯ СЛУЖБИ В ПОЛІЦІЇ США

Boston Dynamics – це провідна американська інженерна компанія, яка випускає роботів-собак та іншу робототехніку з 1992 року. У 2019 році отделение полиции штата Массачусетс стало першим правоохранительным учреждением в США, которое использовало в работе робота Boston Dynamics под названием Spot. Як повідомляє нам видання Wbur News Spot, як і інші роботи відділу, використовувався як «мобільний пристрій віддаленого спостереження», щоб надавати військовослужбовцям зображення підозрілих пристроїв або потенційно небезпечних місць, наприклад, де може ховатися озброєний підозрюваний.

«Технологія роботів є цінним інструментом для правоохоронних органів, оскільки вона здатна інформувати про потенційно небезпечне середовище», – написав речник поліції штату Девід Прокопю. Особливістю Spot є те, що це робот, схожий на собаку, який працює без підзарядки півтори години, рухається зі швидкістю до 5,8 км/год, а також має вантажопідйомність до 14 кг і витримує температуру від –20 °C до 45 °C. Також, він має 360-градусну камеру для слабкого освітлення та руку.

За 2021 рік "робокон" використовувався у двох операціях. У першому випадку, була операція з порятунку заручників, тоді злочинці захопили людей проти їхньої волі і утримували в одній з квартир. Spot, оснащеного камерою і ліхтарями, запустили всередину приміщення, в результаті, все обійшлося без жертв, а злочинці просто втекли.

Другий випадок використання був при затриманні злочинця робопес використовувався у ролі спостерігача.

Ще однією відмінністю Boston Dynamics з їхнім творінням Spot від інших компаній постачальників робототехніки на службу в поліцію є те, що договір компанії та поліції виключає використання робота як зброї, тому він здається в оренду, а не продається. За словами віце-президента Boston Dynamics щодо розвитку бізнесу Майкла Перрі, це зроблено для того, щоб компанія могла відкликати робота, якщо виявить порушення договору.

Як повідомляє нам видання DW після успішного використання роботів Spot від компанії Boston Dynamics у США, Нідерланди перші в Європі придбали собі на службу роботів-собак для виконання ними

завдання-бути розвідниками у нарколабораторіях, для захисту особового складу підрозділів спецназу та звичайних громадян від нападу озброєних злочинців або від ураження отруйними речовинами.

Для цього, Spot оснащений спеціальними датчиками та відеокамерами, які транслюють всю інформацію в режимі реального часу на екран оператора.

Отже, підводячи підсумки можна сказати про те, що залучення інноваційних технологій в діяльності поліції не лише підвищує ефективність роботи поліцейських, а також й збільшує рівень захисту населення і особового складу.

Консультант з мови **Н. В. Краснова**

УДК 351.74:001.895](100)(06)

Руслан ШЕПЕЛЕНКО

Харківський національний університет внутрішніх справ

КРАДІЖКА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Більш відомий як піратство, Інтернет рясніє книгами, музикою, фільмами тощо, які були незаконно отримані та доступні для безкоштовного завантаження. Незважаючи на те, що деякі люди кажуть, піратство не є злочином без жертв. Мало того, що художники та творці програють, але багато незаконних завантажень також містять приховані шкідливі програми, які можуть знищити ваш комп'ютер. Оскільки онлайн-простір стає переповненим, хмарні обчислення стають масовими, а майже все, що знаходиться в Інтернеті, крадіжка інтелектуальної власності стала простішою, ніж будь-коли.

Інтелектуальною власністю можуть бути фільми, музика, вміст в Інтернеті, програмне забезпечення тощо. Ви можете розглядати IP як творіння, а не як фізичні продукти. Але це не означає, що збитки менші, ніж інші види крадіжок. За даними Комісії з крадіжки американської інтелектуальної власності, збитки від крадіжки інтелектуальної власності оцінюються в сотні мільярдів доларів на рік. Крадіжка інтелектуальної власності – це крадіжка, яка викрадає ідею, творчий вираз чи винахід у окремої особи чи компанії. Крадіжка IP може стосуватися того, що хтось викрадає патенти, авторські права, торгові марки або комерційні таємниці. Це включає назви, логотипи, символи, винаходи, списки клієнтів тощо. Випадки крадіжки інтелектуальної власності є надзвичайно поширеними та вимагають розумного програмного забезпечення для управління інтелектуальною власністю, щоб уникнути. Більшість справ про крадіжку інтелектуальної власності

вважаються федеральними (тому федеральними злочинами). Компанії або особи, які можуть ідентифікувати, хто вкрав їх ІР, можуть притягнути їх до суду, а в деяких випадках до злочинців можуть бути накладені серйозні покарання. Сюди входять штрафи, позбавлення волі, цивільні звинувачення, призупинення дії ліцензій тощо.

Якщо хтось вкрав вашу інтелектуальну власність, ви можете зробити кілька кроків, щоб виправити ситуацію. У більшості випадків перше, що потрібно зробити, це попросити людину або компанію, яка вкрала у вас, припинити використання вашої ІР-адреси. Зрештою, крадіжка ІР є злочином, тому особа може погодитися негайно припинити використання ІР. У деяких випадках крадіжка ІР є ненавмисною (наприклад, якщо термін дії ліцензії закінчився). У складніших випадках крадіжки інтелектуальної власності вам, можливо, доведеться звернутися до суду. Зазвичай це починається з того, що адвокат надсилає лист про ймовірні злочини. У багатьох випадках проблема зупиняється на цьому. Якщо це не так, вам, можливо, доведеться перейти до справжнього позову.

У сучасному світі після COVID-19 загрози та атаки кібербезпеці стрімко зростають. Настав час, коли компанії повинні переконатися, що їх ІР захищена від третіх сторін і тих, хто хоче отримати викуп за ІР-адресу за значну плату. 2022 рік деякі називають роком кібербезпеки. Оскільки працівники переходять на моделі роботи з дому, уразливості VPN експлуатуються, і компанії не можуть встигати за порушеннями безпеки, з якими вони стикаються. З огляду на це, атаки програм-вимагачів продовжують зростати, і підприємства виплачують великі суми, щоб повернутися до нормальної роботи. Використання програмного забезпечення для управління інтелектуальною власністю допомагає компаніям відстежувати свої ІР (зокрема програмне забезпечення, ліцензії тощо).

Консультант з мови **В. В. Кочина**

УДК 351.74:001.895](100)(06)

Тетяна ШЕПІЛОВА

Харківський національний університет внутрішніх справ

НАЙБІЛЬШ АКТУАЛЬНІ АРГУМЕНТИ СУЧАСНОГО РУХУ В ЮРИДИЧНІЙ ГАЛУЗІ

Інновації в галузі права більше не є тенденцією чи просто рекламою, а є відчутною та нагальною потребою. Юридичні фірми та корпоративні консультанти перебувають на роздоріжжі, оскільки зміни

в правовому ландшафті за останні кілька десятиліть не дозволяють їм вести свою діяльність у звичайному режимі. У юристів є вибір: йти на цій хвилі або ризикувати втратити шанс зіграти у вищій лізі завтрашньої юридичної галузі.

По всій Європі значні зміни в цивільній та комерційній сфері змушують юридичні фірми та внутрішніх юристів трансформуватися та адаптуватися до цієї нової екосистеми. Великі та відомі юридичні фірми все ще залишаються на вершині піраміди. Однак деякі відносно нові фірми та легальні технологічні компанії відіграють все більш помітну роль на ринку. Як для тих, хто займає посаду, так і для нових агентів, інновації мають значення. Якщо всі юристи хочуть залишатися актуальними в цьому новому ландшафті, вони повинні чітко розуміти, чому інновації в праві мають значення — розуміння, яке виходить далеко за межі оцінки галузу. Нижче наведено деякі з найбільш суттєвих причин останніх змін у юридичній галузі.

Юридична робота минулого більше не ріже її. Незалежно від того, чи ми говоримо про клієнтів юридичної фірми чи внутрішніх клієнтів підприємства, жодне з них не буде продовжувати приймати роботу на тій же основі, що й десять років тому. Це питання не тільки в оплачуваних годинах, а й в ефективності. Жоден клієнт не зацікавлений у тому, щоб пробиратися крізь туман гонорарів, виходячи з іншого боку з чималим рахунком і головним болем. Нині десятки юридичних постачальників пропонують однакові знання та якість роботи, але ті, які виживуть, можуть забезпечити певну винагороду своїм клієнтам.

У молодих юристів зовсім інші цілі. Клієнти життєво важливі, але в юридичному секторі головне таланти. Наступне покоління юристів – це ті, хто допоможе нам подолати цифрове цунамі. Жодне інше покоління в історії не було настільки близьким до технологій. Будучи вихідцями з цифрових технологій, вони найкраще допомагають компаніям адаптуватися, розвиватися та залишатися актуальними зараз і в майбутньому.

Технологія змінила внутрішні процеси. Юристи називали себе ремісниками чи ремісниками. Ті, хто все ще так думає, будуть витіснені з легального ринку. Право – це вже не мистецтво – це наука.

Нові агенти забирають «шматочок пирога». Юридичний ринок більше не є виключною сферою діяльності юристів. Нові юридичні фірми поєднують як юридичний, так і технічний персонал, щоб краще зрозуміти потреби клієнтів і запропонувати найбільш відповідне рішення.

Не забуваймо, що галузь сповнена можливостей. Незважаючи на те, що юридичний ринок надзвичайно зрілий, ми бачили, як юридичні

фірми та генеральні юрисконсульти з найбільшою проблемою працюють і щороку впроваджують нові продукти та послуги. Незалежно від місця розташування чи сфери права, юридична галузь прагне до нового змісту та інновацій.

Консультант з мови В. В. Кочина

УДК 351.74:001.895](100)(06)

Сергій ЮДІН

Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ СИСТЕМИ ВИЯВЛЕННЯ ПОСТРІЛІВ У МІСТАХ США

Впроваджена у кількох містах США система виявлення вогнепальних пострілів (СВВП), або Локатор пострілів, — це система, яка показує поліціантам, де щойно був зроблений постріл. Ця нова і така, що все ще вдосконалюється технологія, використовує чутливі аудіо датчики, розміщені по території громади, щоб виявляти постріли та показувати поліціантам точне місцезнаходження. Ця правоохоронна технологія допомагає поліції швидше реагувати на інциденти з вогнепальними пострілами, що дає їй можливість надавати допомогу жертвам і розшукувати підозрюваних. Технологія СВВП може зробити громади набагато безпечнішими, особливо в районах, де не вистачає поліціантів для цілодобового патрулювання.

Система майже миттєво показує місце пострілу зі зброї з точністю до 25 метрів (82 фути). Технологія Локатора пострілів, яка вже використовується поліціантами в кількох містах США, використовує стратегічно розміщені аудіо датчики, які передають інформацію про місце пострілу поліціантам, які знаходяться поблизу, що дозволяє швидко реагувати. Система, установка та експлуатація якої коштує 1,5 мільйона доларів на рік, також достатньо розумна, щоб передбачити, де можуть відбутися наступні постріли, що дозволяє поліціантам підходити до ситуації з належною обережністю та застосуванням підтримки.

Локатор пострілів переважно використовується в кольорових громадах, які вже непропорційно несуть тягар інтенсивної присутності поліції. Поліція заявляє, що вона вибирає райони для розгортання на основі того, де найбільше стрілянини, але з цим є кілька проблем. По-перше, помилкові тривоги Локатора пострілів відправляють поліцію в численні поїздки (у Чикаго, понад 60 разів на день) у громади без будь-яких причин та у підвищеній готовності, очікуючи потенційного зіткнення з небезпечною ситуацією. По-друге, методологія Локатора

пострілів, що використовується для надання доказів проти обвинувачених у кримінальних справах, не є прозорою і не була перевірена експертами, чи іншим чином незалежно оцінена. Це просто неприпустимо для даних, які використовуються в суді. Нарешті, ефективність технології Локатора пострілів все ще залишається предметом обговорень, але є сподівання, що Локатор пострілів допоможе поліції скласти точну картину того, наскільки активна зброя в містах.

*Науковий керівник **Олександр Олішевський***

УДК 351.74:001.895](100)(06)

Уляна ЯНКОВСЬКА

Харківський національний університет внутрішніх справ

ВІРТУАЛЬНА РЕАЛЬНІСТЬ У НАВЧАННІ ПРАЦІВНИКІВ ПОЛІЦІЇ

Чомусь вважається, що світ майбутнього буде вільним від злочинності. Але чи дійсно настане час, коли можна буде розкрити будь-який злочин і не буде такого злочину, якому не можна було б запобігти? Кілька років тому навіть не йшлося про ідею навчання правоохоронців за допомогою віртуальної реальності. Сьогодні віртуальна реальність досягла високого рівня розвитку, і технологія набула поширення у багатьох професіях. Ці технології навчання можна використовувати для безпечного професійного розвитку, щоб уникнути реальних ризиків у майбутньому. Правоохоронні органи США проводять спеціальні тренінги з використанням віртуальної реальності. Такі навчання допомагають співробітникам поліції підготуватися до непередбачуваних оперативних сценаріїв.

Поліцейські можуть опинитися у віртуальному торговому центрі чи державній школі у ситуації, пов'язаній із захопленням заручників. При цьому відпрацьовуються різні бойові сценарії, засновані на реалістичних подіях. Віртуальна реальність дозволяє поліцейським відпрацьовувати різні сценарії в режимі реального часу та взаємодіяти з віртуальними об'єктами, у тому числі з партнерами. Для цього потрібно одягнути жилет з датчиками та шолом віртуальної реальності. Усі дії поліції фіксуються для подальшого аналізу.

Конструкція одночасно поєднує в собі відео- та фотокамеру, а також навігаційний пристрій. Головною особливістю окулярів віртуальної реакції є створення віртуального екрана. Пристрій нагадує

сонцезахисні окуляри з невеликим потовщенням дужок, у яких встановлені комп'ютерні чіпи. Завдяки цьому поліцейські можуть отримати додатково необхідну інформацію. Наприклад, якщо перевіряється вулиця, пристрій покаже кількість машин на стоянці. Якщо поліцейський наведе окуляри на номер автомобіля, на екрані можуть з'явитися дані про крадіжку автомобіля.

Використання віртуальної реальності відкриває нові можливості для поліцейських. Для роботи з сучасними пристроями віртуальної реальності не потрібні глибокі знання комп'ютерних технологій, що робить їх легкими у освоєнні. Тому дедалі більше країн активно впроваджують технології доповненої та віртуальної реальності в програми підготовки поліцейських.

Науковий керівник Г. М. Сорокіна

Наукове видання

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НА СЛУЖБІ ПРАВОПОРЯДКУ (зарубіжний досвід)

Збірник тез доповідей учасників
XXIII Міжнародної студентської
науково-практичної конференції
іноземними мовами,
присвяченої 30-річчю кафедри іноземних мов

12 квітня 2022 року, м. Харків, Україна

Англійською, німецькою, французькою та українською мовами

Відповідальні за випуск: *О. О. Статівка*
Комп'ютерне верстання: *А. О. Зозуля*

Формат 60x84/16. Ум. друк. арк. 14,47. Обл.-вид. арк. 13,74.

Видавець і виготовлювач –
Харківський національний університет внутрішніх справ,
просп. Л. Ландау, 27, м. Харків, 61080.
Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.