

Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА:
АКТУАЛЬНІ ПИТАННЯ ТА ІННОВАЦІЇ**

*Матеріали Міжнародної
науково-практичної конференції*

(м. Дніпро, 4 листопада 2021 р.)

Дніпро
2021

УДК 33+004+4+35
Е40

*Схвалено науково-методичною радою
Дніпропетровського державного університету
внутрішніх справ протокол № 3 від 18.11 2021)*

Е 40 Економічна та інформаційна безпека: актуальні питання та інновації : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 4 листоп. 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 399 с.

ISBN 978-617-8032-40-1

Збірник містить матеріали однойменної міжнародної науково-практичної конференції. У заході взяли участь науковці, викладачі та здобувачі вищих навчальних закладів та наукових установ України і зарубіжжя, а також фахівці-практики правоохоронних органів. Тематика публікацій охоплює актуальні питання економічної та інформаційної безпеки.

Матеріали конференції можуть бути використані в науково-дослідній роботі та навчальному процесі спеціалізованих ВНЗ, а також у законотворчості та правоохоронній діяльності.

РЕДАКЦІЙНА КОЛЕГІЯ

д-р. юрид. наук, доц., Засл. юрист України **Андрій ФОМЕНКО** (*голова*); д-р юрид. наук, проф., Засл. юрист України **Лариса НАЛИВАЙКО** (*заст. голови*); канд. екон. наук, Засл. економіст України **Олександр СИДОРОВ**; канд. юрид. наук, проф. **Едуард РИЖКОВ**; канд. техн.наук, доц. **Андрій ГРЕБЕНЮК**; канд. екон. наук **Світлана ТЮТЧЕНКО**; канд. техн. наук, доц. **Світлана НАСОНОВА** (*відп. секретар*).

ISBN 978-617-8032-40-1

© Автори, 2021
© ДДУВС, 2021

З М І С Т

ТЕЗИ ВИСТУПІВ

Glavan B.

About the coherence of the legal provisions in the field
of special investigations, criminal law and criminal procedural laws
relating to the protection of the investigator under coverage 20

Klinarytskyi I.I.

Changing the patterns of research on language rights problems:
first draft on the new method of digital research 23

Marinov A.T., Slavyanska V.K.

Indicators for measuring economic security and innovations 27

Popescu G.-D.

Special techniques for surveillance
and investigation regulated by the Romanian Law 30

Urbanec J., Junková D.

Analytical standards in the legislative process (ria) as a tool
for increasing efficiency of the public sector in the czech republic 32

Албул С. В.

Категорії «розвідувальна інформація» та «інформація розвідки»
в оперативно-розшуковій діяльності Національної поліції України 37

Амеліна А. С.

Поняття та чинники інформаційної безпеки 39

Архипенко Т. А.

Роль держави у забезпеченні економічної безпеки підприємств 41

Бабакін В. М.

Окремі аспекти використання інформаційно-аналітичного
забезпечення оперативними підрозділами щодо протидії злочинам,
що вчиняються молоддю 44

Байсеитов Б. Т. Особенности теневого интернета – deep web и dark net	46
Бекишев А. К. Некоторые вопросы реализации концепции «Киберщит Казахстана»	52
Бобиль В. В. Плив корпоративного управління на економічну безпеку акціонерного товариства	57
Бочковий О. В. Ефективність інформатизації антикорупційної діяльності в Україні	59
Бугорська М. Є. Актуальні проблеми використання інформаційних технологій у сфері запобігання та протидії домашньому насильству	62
Бурбело О. А., Бурбело С. О. Інформаційна безпека суб'єктів бізнесу	64
Варяниченко О. В., Госалов Ю. С. Формування управлінських рішень щодо економічної безпеки АТ «Нікопольський завод феросплавів» на основі SWOT-аналізу	70
Варяниченко-Гутовская А. О. Влияние финансовых рисков на экономическую безопасность предприятия	72
Вишня В. Б. Забезпечення економічної безпеки засобами патентної діяльності	74
Головін Д. В. Особенности та порядок використання електронних документів у процесі доказування злочинів у сфері обігу наркотичних засобів	77
Головкова Л. С., Рипюк Д. П. Організація захисту комерційної таємниці на підприємстві	81
Горященко Ю. Г. Господарсько-інституційне забезпечення інноваційної політики держави	83

Гребенюк А. М.

Кіберзлочинність в Україні 85

Дараган В. В.

Деякі проблеми нормативно-правового забезпечення діяльності Бюро економічної безпеки України 88

Демко І. І.

Переваги автоматизації системи бухгалтерського обліку підприємства 90

Долженков О. Ф., Корнієнко М. В.

Імплементация міжнародного досвіду у сфері протидії злочинам щодо дітей: інформаційний аспект 93

Долженков О. Ф., Чебан О. Є.

Деякі аспекти застосування на практиці електронних доказів 98

Дронь М. А.

Система управління ризиками як елемент економічної безпеки банку 101

Дубровіна В. В.

Удосконалення методичного забезпечення інформаційної підготовки фахівців Національної поліції України 103

Ефременко Е. М.

О праве на изображение сотрудника органов внутренних дел в контексте обеспечения и защиты гражданских прав 105

Зачек О. І.

Загрози інформаційної діяльності антивакцинаторів у період пандемії COVID-19 108

Зачосова Н. В.

Управління фінансово-економічною безпекою як сучасний елемент менеджменту суб'єктів господарювання 110

Каркоцький І. О.

Інформаційне забезпечення реалізації принципу об'єктивності та повноти дослідження в судово-експертній діяльності 112

Карчевський М. В.

Протидія злочинності в Україні у форматі data science 114

Каткова Т. Г.

Адміністративна відповідальність за порушення
законодавства у сфері захисту персональних даних 120

Климюк І. М.

Роль інформаційних технологій у забезпеченні
економічної безпеки України 123

Коваленко А. О.

Роль кадрового потенціалу суб'єктів господарювання
в управлінні їх економічною безпекою 124

Коваль О. В.

Фактори впливу на вибір стратегії управління
економічною безпекою суб'єкта господарювання 126

Користін О.Є.

Ризик-орієнтований підхід у стратегічному
вимірі внутрішньої безпеки України 128

Корнейко О. В., Школьніков В. І.

Досвід освітньо-наукової діяльності Національної академії
внутрішніх справ у сфері кримінальної аналітики 131

Косиченко О. О.

Використання технологій візуалізації
даних у боротьбі зі злочинністю 134

Крамаренко Ю. М.

Окремі тенденції у сфері організованої
злочинності (за матеріалами Європолу) 136

Куценко Д. М.

Передумови використання комплексного підходу
до формування механізму управління економічною безпекою 138

Кушнір Л. П., Гримак О. Я., Калайтан Т. В.

Фактори формування тіньової економіки в індустрії гостинності 141

Легеза Є. О.

Правове регулювання поняття національної безпеки України 144

Лізунов С. І.

Активне придушення звукової інформації 146

Лопатка К. А.

Аналіз взаємозв'язку стратегії економічної безпеки
й загальної стратегії підприємства 148

Марценюк Л. В.

Напрями підвищення економічної безпеки
залізничного транспорту України 149

Матусевич О. О., Постільженко Г. С.

Джерела фінансування капітальних вкладень АТ «Укрзалізниця» 151

Махницький О. В.

Ризики використання старих операційних
систем на прикладі Windows XP 153

Мироненко М. А., Король Р. М.

Аналіз деяких показників кадрового та фінансового
стану науково-дослідної установи державної форми
власності у 2018 – 2 кв. 2021 р. 158

Мирошніченко В. О.

Відеотехнології: можливості та проблеми використання 160

Мішкевич Ж. В., Рудой К. М.

Впровадження інформаційної підсистеми «Custody Records»
у діяльність Національної поліції України 163

Мордвинцев М. В., Хлестков О. В., Ницюк С. П.

Технічні проблеми, пов'язані зі стрімким розвитком систем
відеоспостереження, і способи їх вирішення 165

Насонова С. С.

Забезпечення безпеки складних систем
з високим ступенем відповідальності 167

Охрименко С. А., Бортэ Г. Р., Черней В. А.

Тень цифровой трансформации 169

Панченко Л. В.

Мультистейкхолдерська модель управління Інтернетом 171

Паршин Ю. І.

Вплив податкових сховищ на економіку держави 174

Пекарський С. П.

Використання інформаційно-аналітичного
забезпечення під час розшуку транспортних засобів
у зв'язку з незаконним заволодінням 176

Пєфтієв Д. О.

Проблемні питання побудови поліцейської діяльності,
що базуються на зборі та аналізі даних (ILP) 180

Покраса К. В.

Актуальні питання використання інформаційних систем
та технологій під час проведення огляду місця події умисного
знищення або пошкодження чужого майна шляхом підпалу 183

Прокопов С. О.

Використання поліцейських квестів у навчальному процесі
Дніпропетровського державного університету внутрішніх справ 186

Прокопович-Ткаченко Д. І.

Новітні технології хмарних інформаційно-технічних систем 193

Разумова Г. В., Усатенко А. Г.

Методи забезпечення економічної безпеки підприємства 196

Рибальченко Л. В.

Кіберзлочинність та її вплив на економічну безпеку країни 198

Рижков Е. В.

Використання інфотелекомунікаційних
технологій у сфері захисту економіки 200

Рижкова С. А.

amber Alert в Україні: система оперативних сповіщень
про зниклих дітей за допомогою facebook 204

Самойленко О. А., Тітуніна К. В.

До питання узагальнення статистичної інформації
з метою протидії кіберзлочинам 207

Санакоєв Д. Т.

Сучасні технології в діяльності поліції: світовий досвід та перспективи впровадження у протидії організованим формам злочинності 210

Сарахман О. М., Сідельник О. П.

Вплив діджиталізації на операційні ризики банків 215

Сеник В. В., Кулешник Я. Ф., Ментинський С. М.

Стан та перспективи розвитку технологій захисту хмарних сервісів 217

Синиціна Ю. П.

Автоматизовані інформаційні системи в правоохоронній діяльності 220

Станіна О. Д.

Вплив пандемії COVID-19 на зміну структури злочинності в Україні та світі 222

Сулейменов А. Д.

Проблемы обеспечения информационной безопасности в Республике Казахстан 224

Телійчук В. Г.

Щодо проблеми оперативно-розшукової протидії незаконному обігу вогнепальної зброї у мережі «Інтернет» 227

Трифорова О. В.

Оцінювання якості життя населення України як складова безпеки держави 231

Тютченко С. М.

Інноваційна складова в економічній безпеці підприємства 233

Тютченко С. М., Бут К. А.

Інформаційна безпека на підприємстві 235

Федчак І. А.

Модель запобігання злочинності «превенція злочинів за допомогою зміни навколишньої інфраструктури» (crime prevention through environmental design – CPTED) 237

Фещенко А. Ю.

Противодействие уголовным рискам криптовалют 239

Фісуненко Н. О.

Цифровізація економіки як суспільне явище 244

Хамініч С. Ю., Коваленко-Марченкова Є. В.

Теоретичні аспекти захисту економічних інтересів держави
в системі національної безпеки 246

Ханькевич А. М., Третьяк О. С.

Оперативно-розшукове прогнозування в діяльності
підрозділів кримінальної поліції 248

Худенко Д. М.

Забезпечення оперативних працівників та інспекторів,
які займаються кримінальним аналізом, інформацією про віртуальні
активи на основі поліцейських інформаційних ресурсів 251

Чобану Г.

Необхідність підготовки спеціалістів в області
кибербезпеки и расширения специализации в современных
условиях кризиса экономического и социального развития 254

Чупілко Т. А.

Комп'ютерні технології як інструмент моделювання
та прогнозування показників економічної безпеки 260

Шаблиста О. О.

Інформаційні технології як інструмент захисту
інформації Національною поліцією України 262

Шелехов А. А.

Обеспечение безопасности перевозок коммерческих грузов
автомобильным транспортом органами полиции Канады и США 263

Шеломенцев В. П., Шаповалова О. В.

Законодавство про загрози дитині у кіберпросторі 269

Шурпенкова Р. К.

Оцінка стану та проблем соціальної безпеки у контексті
взаємозв'язку з економічною безпекою 272

Якименко Ю. М.

Підхід до забезпечення економічної безпеки
підприємства в умовах інноваційного розвитку 274

Ящук В. І.

Використання інформаційних технологій під час визначення
рівня економічної безпеки підприємств ритейлу 277

КУРСАНТИ ТА СТУДЕНТИ

Janine Al-Shargabi

Line 102 – review from zhanin 280

Байрак К. С., науковий керівник – Рижков Е. В.

До питання правового регулювання інформаційної безпеки в Україні 282

Барановська О. В., Михайлов Д. Є., науковий керівник – Кононова І. В.

Принципи забезпечення економічної безпеки підприємства 284

Братішко Н. А., науковий керівник – Тютченко С. М.

Інформаційне забезпечення Національної поліції 286

Булдакова А. Є., науковий керівник – Прокопов С. О.

Проблеми використання технічних засобів
працівниками Національної поліції України 288

Волкова А. В.

Фішинг – основа кібератак 290

Волчок Є. В., науковий керівник – Ісмайлов К. Ю.

Експлуатація вразливостей в мобільній криміналістиці IOS-пристроїв 292

Гнатко А. Р.

Подолання опору до програм аналізу злочинності
(огляд спеціальної літератури США) 296

Голубєва Д. В., науковий керівник – Прокопов С. О.

«Групи смерті»: інформаційна безпека та її забезпечення
оперативними підрозділами Національної поліції України 298

Добош В. В., науковий керівник – Неклеса О. В.

Значення фінансової безпеки у забезпеченні
економічної безпеки держави 300

Волчок Є. В.,

здобувач 2-го курсу магістратури
Одеського державного
університету внутрішніх справ,
співробітник відділу security analyst
ТОВ «Група інформаційної безпеки
«ФС ГРУП», м. Одеса

Науковий керівник – Ісмайлов К. Ю.,

старший науковий співробітник НДІЛ
з проблемних питань кримінального
аналізу Одеського державного
університету внутрішніх справ,
начальник 5-го відділу 3-го управління
ДКП НПУ, кандидат юридичних наук,
доцент, підполковник поліції

ЕКСПЛУАТАЦІЯ ВРАЗЛИВОСТЕЙ В МОБІЛЬНІЙ КРИМІНАЛІСТИЦІ IOS-ПРИСТРОЇВ

Внаслідок розвитку інформаційних технологій та різноманітної електронно-обчислювальної техніки, таких як комп'ютери, ноутбуки, мобільні телекомунікаційні пристрої, з'являються нові методи та заходи захисту інформації від несанкціонованої передачі та витоку її.

В багатьох пристроях як первинний захист використовується метод шифрування накопичувача різними засобами: як запроваджений розробником операційної системи (Google або Apple, якщо ми говоримо про мобільні пристрої), так і безпосередньо виробниками пристроїв.

В нашому випадку мова буде йти безпосередньо про витяг і подальший криміналістичний аналіз отриманої інформації з Apple пристроїв на основі операційної системи iOS (iPhone, iPod) та iPadOS (iPad), їх методи захисту Secure Enclave Protection (TouchID, FaceID), DAP та їх можливі вразливості як апаратного, так і програмного характеру. Оскільки пристрої виробництва Apple досить поширені серед населення (приблизно 30–40 % від загальної кількості смартфонів на території України), тому має сенс звернути увагу саме на цей прошарок, адже на сьогодні є багато методів щодо отримання інформації з пристроїв на операційній системі Android (як апаратними методами, так і за допомогою програмних властивостей безпосередньо від розробників цих самих пристроїв або операційної системи). Наприклад, компанія Samsung розробила власну систему захисту даних Knox, але навіть вона беззахисна в деяких випадках. Нижче наведені порівняльні таблиці 1 і 2 з кількістю знайдених вразливостей на Android та iOS за весь час [1, 2]:

Таблиця 1

Кількість знайдених вразливостей в Android

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2009	5	3							1			
2010	1	1	1									
2011	9	1	1		1		1		4	1	3	
2012	7	5	3	2						1		1
2013	4		1	1	1				1	1	1	
2014	12	2	4	1		1			1	2	1	1
2015	95	46	49	50	37				13	14	17	
2016	500	104	72	91	38				47	96	236	
2017	840	86	206	170	32			1	30	113	36	
2018	609	32	84	143	12	2	1	2	17	63	3	
2019	491	37	107	41	24	3		1	39	22	1	
2020	859	46	97	104	27	9		5	148	97	3	
2021	394	17	44	35	33	2		3	40	10	6	
Total	3826	380	669	638	205	17	2	12	341	420	307	2
% of all		9.9	17.5	16.7	5.4	0.4	0.1	0.3	8.9	11.0	8.0	

Отже, метою нашого дослідження є використання різноманітних програмних та апаратно-програмних методів і способів для можливості отримання інформації з пристроїв Apple для проведення оперативно-розшукових заходів та проведення криміналістичного аналізу отриманої інформації. А саме приклад буде наведений на основі застосування мініатюрного комп'ютера Raspberry Pi 4 [2].

Цей пристрій завдяки розміру, форм-фактору та автономності дозволяє зручно переносити буквально в кишені і використовувати його під час проведення слідчих дій, виїзду до місця скоєння правопорушення, або під час затримання підозрюваного суб'єкта без застосування ПК, ноутбука або іншого типу ЕОМ.

Таблиця 2

Кількість знайдених вразливостей в iOS

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2007	1		1	1								
2008	1	1	1									
2009	10	2	3	2	2				2	3		
2010	20	11	9	5	3				4	2	1	
2011	83	52	7	6	6		5		7	13	1	
2012	155	114	70	67	60		8		15	9	1	
2013	95	57	50	42	46		4		17	9	1	
2014	120	50	51	35	33			1	20	24	4	
2015	386	232	211	184	191			5	44	63	13	1
2016	168	113	79	81	81		3		8	42	11	
2017	388	241	222	210	194		14		39	63	5	
2018	125	63	63	55	50		1		19	19	2	
2019	354	9	101	101	167	2	14			26	5	
2020	305	17	141	57	60		8	2	6	13	5	
2021	244	14	118	22	26		5	3	7	6	7	
Total	2455	976	1127	868	919	2	62	11	188	292	56	1
% of all		39.8	45.9	35.4	37.4	0.1	2.5	0.4	7.7	11.9	2.3	0.0

На сьогодні для експлуатації цього методу підтримуються пристрої, які мають апаратну вразливість checkm8, виявлену у вересні 2019 року [3], а саме від моделі Apple iPhone 5S до iPhone X з декількома застереженнями. Етапи отримання інформації з досліджуваного пристрою:

1. Для початку роботи необхідно на пристрій Raspberry Pi встановити та налаштувати операційну систему зі скриптами, підключити зовнішнє джерело живлення або power bank (підзарядник) та Lightning-кабель для підключення Apple пристроїв.

2. Досліджуваний пристрій попередньо необхідно перевести у режим DFU (Device Firmware Upgrade).

3. І залишається тільки підключити до пристрою Raspberry Pi, після

чого буде запущений автоматизований процес експлуатації вразливості checkm8 та збір усієї можливо доступної інформації з пристрою.

Оскільки більша частина інформації знаходиться у зашифрованій області пам'яті та оберігається в тому числі засобами SEP (Secure Enclave Protection), а сам засіб на цей час в стадії PoC (Proof of Concept), можна отримати лише не зашифровану інформацію, яка доступна в стані BFU (Before First Unlock).

Отже, за допомогою цього методу можна автоматизовано отримати таку інформацію:

- дані про Wi-Fi мережі, до яких підключався пристрій + геопозиція по BSSID точок доступу;
- облікові записи на пристрої (iCloud, Apple ID, поштові скриньки, тощо);
- дані ОС (версія, номер збирання, інша технічна інформація);
- дані про встановлені раніше SIM (номер, ICCID);
- дані статусу функції «Екранного часу»;
- заблоковані (додані в чорний список) мобільні номери;
- облікові дані, які використовуються для входу в FaceTime, iMessage;
- дата та спосіб створення (хмара або локально на ПК) останнього бекапу, підключення до ПК (назва самого ПК і версія iOS пристрою).

Вся отримана інформація зберігається у вигляді архіву безпосередньо на накопичувачі MicroSD, з якої і виконується загрузка ОС, або на зовнішній USB накопичувач для більш зручного подальшого дослідження.

Надалі планується багато нововведень та доопрацювань для більшої автоматизації, структуризації і впровадження роботи з тимчасовими даними, додатків з динамічними GUID і, найголовніше, зі зв'язкою ключів (keychain-2.db).

Бібліографічні посилання

1. CVE Details. URL: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224.
2. CVE Details. URL: https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49.
3. Шах и мат! Как устроен нашумевший эксплоит checkm8 и как им воспользоваться. URL: <https://xakep.ru/2019/11/21/checkra1n>.
4. Raspberry Pi 4 URL: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b>.