

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



**Вітальне слово
ректора Дніпропетровського державного
університету внутрішніх справ
ФОМЕНКА АНДРІЯ ЄВГЕНОВИЧА,
доктора юридичних наук, доцента,
заслуженого юриста України,
полковник поліції**

Шановні учасники конференції! Радий Вас вітати від імені науково-педагогічного колективу Дніпропетровського державного університету внутрішніх справ та від себе особисто на Міжнародній науково-практичній конференції «Економічна та інформаційна безпека: актуальні питання та інновації». Статус заходу є міжнародним і це підтверджує актуальність питань, що нами розглядаються.

Сучасний вік – вік інформації не тільки відкриває можливості, а й ставить нові завдання, та потребує вирішення нових проблем. Тому необхідно адекватно реагувати на подібні виклики. Можна сміливо стверджувати, що економічна та інформаційна небезпеки становлять один з найбільш небезпечних видів загроз, і свідченням цього є постійне обговорення проблем економічної та інформаційної безпеки як науковою спільнотою, практиками, так і на офіційних зустрічах на найвищому політичному рівні.

Наш університет має певні досягнення в цьому напрямі. Останнім часом створено відповідну кафедру та факультет підготовки курсантів для підрозділів стратегічних розслідувань Національної поліції за спеціалізацією «фінансово-економічна безпека». Споруджено спеціалізований полігон для відпрацювання фабул з документування та розкриття злочинів в економічній сфері. Відкриті нові спеціальності для підготовки студентів у сфері менеджменту за спеціалізацією «економіко-фінансова безпека» й економіки за спеціалізацією «захист економіки».

Зважаючи на сучасні реалії, тема нашого обговорення є надзвичайно актуальною, глибокою і водночас складною.

Складність і глобальний характер завдань вимагають розробки ґрунтовного наукового супроводження і консолідації зусиль представників наукової спільноти.

Тож з огляду на зазначене мета сьогоднішнього наукового заходу – обговорити такі питання:

- використання інформаційних технологій в діяльності поліції;
- безпека в інформаційній та економічній сфері;

– сучасний стан, проблеми та перспективи розвитку фінансової та економічної безпеки підприємств, регіонів, суспільства.

Саме для отримання відповідей на ці проблемні питання та удосконалення практичних і теоретичних навичок проводиться цей захід.

Завдяки присутності на заході фахівців різних сфер науки і практики, а саме: економіки, менеджменту, інформаційних технологій, економічної та інформаційної безпеки, юриспруденції, бізнесу та правоохоронних органів ми маємо виняткову змогу перейняти позитивний досвід у зазначеній сфері, а також поділитися власним досвідом.

Переконаний, що наукова дискусія під час обговорення визначених питань матиме глибокий та плідний характер і сприятиме розвитку вітчизняної науки, подальшому підвищенню рівня протидії злочинності в економічній та інформаційній сферах.

Від імені оргкомітету конференції щиро дякую вам за те, що знайшли час взяти участь у конференції з цієї, безперечно актуальної на сьогодні, проблематики.



Вітальне слово
т.в.о. начальника Департаменту
інформаційно-аналітичної підтримки
Національної поліції України,
кандидата юридичних наук
ТИМЧЕНКА ЛЕОНІДА ЛЕОНІДОВИЧА

Дозвольте мені від імені колективу Департаменту інформаційно-аналітичної підтримки поліції України привітати вас з проведенням Міжнародної науково-практичної конференції «Економічна та інформаційна безпека: питання та інновації».

Варто зауважити, що розвиток публічних послуг дозволяє провідним країнам світу в цій сфері не лише підвищувати швидкість та якість обслуговування, але й суттєво економити бюджетні кошти та час держави на обслуговування громадян.

У 2020 році, порівняно з попереднім роком, міжнародна пропускна здатність Інтернету зросла на 35 %, приблизно з 450 до 600 Тбіт/с. З 2014 року зростання відбувалося майже тричі.

Кількість користувачів Інтернету у світі досягла майже 5 млрд осіб, що становить приблизно 63 % від загальної кількості світового населення. За 2020 рік в Україні кількість користувачів зросла з 19 до 26 млн, або з 45 % до 58 % населення. До 2023 року в уряд України має намір приєднати 95 % соціальної інфраструктури до Інтернету.

Говорячи про зростання даних, можна відмітити, що тільки ютуб

завантажується до 300 годин відео. Однак оцінки дозволяють припустити, що тільки 0,5 % усіх даних коли-небудь аналізуються та використовуються.

Стрімке поширення цифрових технологій робить «цифрові» навички людей одними з основних. Цифровізація та робота з даними зараз головні тренди на загальному ринку праці. Тобто вміння працювати з цифровими технологіями поступово стає необхідним для більшості спеціальностей. Для всебічної цифровізації ДІАП розбудовує середовище інформаційних технологій для користувачів баз даних, цифрових сервісів, телекомунікаційних послуг та радіозв'язку.

Сподіваюсь, що під час обговорень та наукових дискусій учасниками конференції буде розроблено нові методи та підходи створення якісного цифрового сервісу. Розроблені рекомендації сприятимуть розробленню законодавства та практики його застосування.



**Вітальне слово т.в.о. начальника
Департаменту кримінального аналізу
Національної поліції України
ХУДЕНКА ДМИТРА МИКОЛАЙОВИЧА**

Шановний голово організаційного комітету! Шановні члени організаційного комітету та учасники Міжнародної науково-практичної конференції! Щиро вітаємо всіх від імені колективу Департаменту кримінального аналізу Національної поліції України з нагоди відкриття цього заходу! Проведення конференції на міжнародному рівні та заявлені учасниками теми наукових розвідок наголошують на особливій актуальності досліджень питань економічної та інформаційної безпеки.

Вкрай важливою передумовою інновацій у згаданих сферах безпеки залишається наука. Не менш важливою для науки є практика. Ці два феномени взаємозалежні у своєму розвитку і потребують обміну думок між українськими науковими школами, фахівцями й представниками міжнародних організацій та наукових еліт іноземних країн.

Програма нашої конференції містить різноаспектний масив питань, зокрема пов'язаних із кримінальним аналізом. Для Департаменту кримінального аналізу, який також розробляє, впроваджує та застосовує нові методи та напрями здійснення кримінального аналізу, спрямовані на підвищення ефективності протидії злочинності, цей формат конференції є надзвичайно цікавим.

У сучасних умовах світового розвитку, коли, наприклад, економіка зазнала впливу пандемії, назріває чергова науково-технічна революція, обсяг

інформації зростає шаленими темпами, а фізичний світ шукає альтернатив у віртуальному, представники злочинного світу користуються не лише класичними способами вчинення злочинів у зазначених сферах, але й вдаються до нових або досі не бачених способів їх підготовки та вчинення. Саме тому ми змушені постійно підвищувати протидію злочинності.

55 років досягнень Дніпропетровського державного університету внутрішніх справ та якісний склад учасників Міжнародної науково-практичної конференції дають нам міцний фундамент для полеміки та успішного розвитку системного наукового та міждисциплінарного підходу до вивчення проблем економічної та інформаційної безпеки.

Ми сподіваємось, що знання, досвід та пропозиції учасників Міжнародної науково-практичної конференції стануть в нагоді на шляху забезпечення економічної та інформаційної безпеки суспільства.

Бажаємо всім плідної співпраці, вагомих результатів на практиці, творчих успіхів та наукових відкриттів!



**Приветственное слово ректора
Бухарестского университета «ARTIFEX»,
профессора, доктора философии
АЛЕКСАНДРУ-ЛУЧИАН МАНОЛЕ**

Уважаемые коллеги! Для меня большая честь участвовать в качестве представителя Бухарестского университета «ARTIFEX» в престижной конференции по экономической и информационной безопасности, организованной уважаемым Днепропетровским государственным университетом внутренних дел. Тема конференции чрезвычайно важна и актуальна, когда экономическая информация является одним из ключей к управлению политическими отношениями. Развитие (и преимущества) компьютерной обработки информации вместе с расширением сетей сопряжено с некоторыми издержками, одна из которых связана с безопасностью информации, которую необходимо защищать любой ценой. Мы можем согласиться с тем, что после компрометации конфиденциальность информации не может быть восстановлена.

От имени академического сообщества Бухарестского университета «ARTIFEX» выражаю самые искренние пожелания, поздравления и уважение организаторам и участникам конференции. Мы считаем, что усилия исследователей должны быть капитализированы в ценной и полезной базе знаний и собрании передового опыта, что будет способствовать усилению безопасности физических и электронных систем обработки информации.

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

Klinytskyi 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. Особливості 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 антивакцинологів 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
Мирошниченко 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

Пефтієв 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

Дроговоз С. Є., науковий керівник – Ришков Е. В. Позитивні та негативні аспекти використання в діяльності патрульної поліції системи «Цунамі»	302
Еркенов Б. Д., научный руководитель – Жемпиусов Н. Ш. Некоторые вопросы применения информационных технологий в обеспечении экономической безопасности Республики Казахстан	305
Задорожня І. І., науковий керівник – Гребенюк А. М. Кримінальний аналіз у діяльності Національної поліції України	308
Зеленський А. В., науковий керівник – Прокопов С.О. захист персональних даних у кіберпросторі	310
Калашнік Є. О., науковий керівник – Прокопов С. О. Правове регулювання інформаційної безпеки як підґрунтя вільного інформаційного простору в Україні	312
Калюжна А. О., науковий керівник – Косиченко О. О. Ризики використання систем біометричної ідентифікації користувачів	315
Касич Є. Ю., науковий керівник – Прокопов С. О. Поширення кіберзлочинності в сучасній Україні, проблематика та шляхи вирішення	317
Ковбаса М. В., науковий керівник – Верхоглядова Н. І. Економічна безпека підприємства: сутність та ознаки	320
Коляда Д. В., науковий керівник – Паршин Ю. І. Подолання економічної кризи в Україні під час пандемії COVID-19	322
Коптєв О. С., науковий керівник – Прокопов С. О. Тактичний кримінальний аналіз	324
Корінь Д. К., науковий керівник – Прокопов С. О. Проблеми інформаційного захисту підприємств та установ	326
Костюк Ю. А., науковий керівник – Неклеса О. В. Структура й особливості економічної злочинності на споживчому ринку	329

Кочкіна Д. А., науковий керівник – Прокопов С. О. Витік даних як один з основних різновидів кібератак	331
Крися О. Ю., науковий керівник – Паршин Ю. І. Тіньова економіка: причини виникнення	334
Кричун А. Ю., науковий керівник – Косиченко О. О. Перспективи використання інформаційних технологій в юридичній діяльності	336
Кріпак А. Ю., науковий керівник – Прокопов С. О. Сучасний стан та перспективи розвитку інформаційної безпеки Національної поліції України	339
Лагода М. В., науковий керівник – Паршин Ю. І. Економічна безпека держави та підприємства в умовах інноваційного розвитку	341
Лукомська А. А., науковий керівник – Мирошніченко В. О. Кібербезпека віддаленої роботи у сфері бізнесу під час пандемії COVID-19	343
Масоха В. О., науковий керівник – Паршин Ю. І. Страхові резерви та їх збереження	345
Миршака В. С., Перетятко К. О., науковий керівник – Фісуненко Н. О. Суть та структура факторів, що впливають на формування конкурентоспроможності підприємства	347
Моргалюк К. Р., науковий керівник – Рибальченко Л. В. Проблеми шахрайства на підприємстві	349
Морохіна К. Д., науковий керівник – Гребенюк А. М. Основні положення про кримінальний аналіз	352
Нагорна Д. А., науковий керівник – Паршин Ю. І. Інформаційна безпека підприємства як один із головних напрямів безпеки підприємства	354
Недєлков К. Ю., науковий керівник – Ісмайлов К. Ю. Автоматизований аналіз образів файлової системи та збір цифрових доказів кримінального характеру як спосіб запобігання кібератак	356

Неделков К. Ю., здобувач 2-го курсу магістратури Одеського державного університету внутрішніх справ, співробітник відділу research and forensic ТОВ «Група інформаційної безпеки «ФС ГРУП», м. Одеса
Науковий керівник – Ісмайлов К. Ю., старший науковий співробітник НДЛ 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

АВТОМАТИЗОВАНИЙ АНАЛІЗ ОБРАЗІВ ФАЙЛОВОЇ СИСТЕМИ ТА ЗБІР ЦИФРОВИХ ДОКАЗІВ КРИМІНАЛЬНОГО ХАРАКТЕРУ ЯК СПОСІБ ЗАПОБІГАННЯ КІБЕРАТАК

Витонченість хакерських інструментів зростає мало не щодня. Якщо кілька років тому шкідливе програмне забезпечення (ПЗ) найчастіше купувалося у самого розробника, який міг зникнути відразу після продажу, не гарантуючи працездатності продукту, то сьогодні практично будь-яка людина з мінімальними теоретичними і практичними навичками в комп'ютерній вірусології та кібербезпеці може придбати malware-as-a-service [1] з повною технічною підтримкою, включно з розробкою ботнету під ключ, купівлею доменного імені, орендою сервера, розгортанням контрольної панелі на сервері (далі С&С-сервер) [2], послугою шифрування шкідливого ПЗ або обфускації коду, тестуванням на детектування великою кількістю антивірусних рішень тощо.

За даними міжнародної некомерційної організації «The Spamhaus Project», яка, у тому числі, досліджує активність ботнетів [3] та географічне розташування їхніх С&С серверів, у своєму звіті [4] за 2-й квартал 2021-го року помістило Україну на 8-ме місце у світі за кількістю розміщених С&С серверів зловмисників (рис. 1).

Порівняно з першим кварталом цього ж року – у другому кварталі кількість зафіксованих серверів зловмисників збільшилась вдвічі. Крім того, один з українських хостинг-провайдерів посів п'яту сходинку (рис. 2) у рейтингу найпопулярніших у зловмисників «майданчиків» для розміщення контрольних панелей ботнетів.

Rank	Country	Q1 2021	Q2 2021	% Change Q on Q	Rank	Country	Q1 2021	Q2 2021	% Change Q on Q
#1	United States	338	281	-17%	#11	Czech Republic	-	31	New entry
#2	Russia	195	233	19%	#12	Moldova	29	29	0%
#3	Netherlands	207	168	-19%	#13	Panama	-	16	New entry
#4	Germany	99	117	18%	#13	Canada	26	16	-38%
#5	France	71	92	30%	#15	Malaysia	-	15	New entry
#6	Latvia	31	84	171%	#15	Poland	-	15	New entry
#7	United Kingdom	49	57	16%	#17	Finland	-	14	New entry
#8	Ukraine	22	44	100%	#18	Vietnam	-	13	New entry
#9	Switzerland	59	41	-31%	#18	Turkey	25	13	-48%
#10	Seychelles	29	38	31%	#20	Brazil	20	12	-40%

Рис. 1. Рейтинг країн, в яких були розміщені С&С сервери у 2-му кварталі 2021-го року

Через що ще більше актуалізується питання потенційної загрози та превентивних методів виявлення контрольних серверів зловмисників.

Рис.2. Рейтинг хостинг-провайдерів, на яких зафіксовано розміщення С&С серверів у 2-му кварталі 2021-го року

Метою дослідження є розробка алгоритму виявлення та дослідження контрольних серверів ботнетів завдяки автоматизованому аналізу файлової системи цих та збір криміналістичних цифрових доказів.

Rank	Q1 2021	Q2 2021	% Change	Network	Country
#1	35	82	134%	pq.hosting	Russia
#2	53	74	40%	google.com	United States
#3	21	68	224%	serverion.com	Netherlands
#4	51	56	10%	ovh.com	France
#5	23	53	130%	itldc.com	Ukraine
#6	-	49	New Entry	nano.lv	Latvia
#7	131	48	-63%	privacyfirst.sh	Germany
#8	-	47	New Entry	mgnhost.ru	Russia
#9	19	46	142%	hetzner.de	Germany
#10	-	40	New Entry	baxet.ru	Russia
#11	-	35	New Entry	ipjetable.net	France
#12	45	29	-36%	cloudflare.com	United States
#12	-	29	New Entry	digitalocean.com	United States
#14	-	28	New Entry	Internet.it	Russia
#15	26	26	0%	alibaba-inc.com	China
#16	-	25	New Entry	hostsailor.com	U. Arab Emirates
#17	-	22	New Entry	microsoft.com	United States
#18	-	21	New Entry	m247.ro	Romania
#19	-	16	New Entry	offshoreracks.com	Panama
#19	-	16	New Entry	mivocloud.com	Moldova

Зловмисники нерідко вдаються до розгортання своїх послуг і сервісів на «білих» чи «сірих» хостингах, що спричиняє фінансові та репутаційні втрати як жертвам шкідливих кампаній, так і самим хостинг-провайдерам.

Найчастіше для розгортання С&С-панелей використовується VPS (Virtual Private Server) або VDS (Virtual Dedicated Server) з т. з. LAMP

конфігурацією (Linux (ОС), Apache (WEB-сервер), MySQL (СУБД – система управління базами даних), phpMyAdmin (вебінтерфейс для адміністрування СУБД)). Ця конфігурація цілком схильна до автоматизації отримання необхідної інформації для проведення аналізу і збору криміналістичних доказів.

Більш детально зупинимось на розробленій нами концепції автоматизованого рішення для аналізу файлових систем підозрілих орендарів VPS/VDS з отриманням цифрових доказів зловмисників, що дозволить як припинити підготовку шкідливої кампанії, так і потенційно встановити наміри і самого зловмисника. Алгоритм ПЗ, який дозволить отримати з C&C-сервера зловмисника таку інформацію (у разі вилучення дампа ОС у хостинг-провайдера з боку правоохоронних органів у межах кримінального провадження або розслідування):

- SQL дампи бази даних та їх структуру;
- лог-файли підключень SSH/RDP протоколів;
- отримання даних про жертви вірусних кампаній;
- отримання даних про зловмисників.

Щодо одержуваної структури бази даних, то за інформацією з відкритих джерел (наприклад, збірника вихідних кодів C&C-панелей деяких троянів-стілерів внаслідок витоку інформації або припинення розробки і підтримки шкідливого програмного забезпечення (далі ШПЗ) хакером (надається для дослідницьких цілей – <https://github.com/threatland/TL-TROJAN>)), зустрічаються порожні «шаблони» баз даних того чи іншого ШПЗ, в якому присутня структура та назва таблиць бази даних. За цими даними можна визначити унікальні особливості і з високою точністю визначити приналежність бази даних до того чи іншого виду ШПЗ безпосередньо за структурою бази даних, тобто створення певних сигнатур.

Отже, проаналізувавши усю згадану вище інформацію, робимо висновок, що для розробки алгоритму виявлення, дослідження C&C серверів та збору цифрових доказів необхідно:

- мінімізація часу обробки дампу до ~10 хвилин (залежності від кількості та обсягу інформації, що знаходиться в дампі ФС та потужності дослідного ПК);
- уніфікування процесу обробки дамтів файлових систем (далі ФС) з різними версіями і родинами ОС (Ubuntu, Debian, Centos, Windows та інші);
- підвищення відмовостійкості для того, щоб на процес і подальшу обробку дамтів не впливали вихід з ладу локального серверу бази даних MySQL завдяки інтеграції можливості діагностики та відновлення БД в разі виникнення помилок;
- створення сигнатур баз даних найчастіших шкідників, які дозволяють категоризувати бази даних і відразу ж виокремлювати потрібну інформацію з потрібних таблиць БД;
- ведення статистики отриманої інформації з кожного дампа і

сумарну кількість отриманої інформації після всього циклу обробки дамів ОС;

- автоматизація роботи за планувальником завдань без участі «ззовні»;

- додавання повного журналювання процесу роботи скрипта і збирати налагоджувальну інформацію в разі якихось несправностей для максимально оперативного вжиття заходів і локалізації проблеми.

Цей проєкт призначений для спрощення і прискорення процедур ідентифікації призначення деяких серверів, на які можуть надходити скарги, а також ті сервери, які можуть використовуватися у вірусних кампаніях зловмисниками.

Бібліографічні посилання

1. Malware-as-a-Service: Who Can Put an End to It? URL: <https://clario.co/blog/malware-as-a-service>.
2. Command and Control [C&C] Server. URL : <https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server>.
3. Ботнет. URL : <https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82>.
4. Spamhaus Botnet Threat Update: Q2-2021. URL : <https://www.spamhaus.org/news/article/813/spamhaus-botnet-threat-update-q2-2021>