Кіберпростір як середовище фінансування тероризму: виклики та методи протидії

Особливості використання кіберпростору для фінансування тероризму

Анонімність

Кіберпростір приваблює терористів анонімністю та глобальністю. Це дозволяє їм здійснювати транзакції, не розкриваючи свою особу.

Криптовалюти

Використання Bitcoin, Ethereum для транзакцій стає все популярнішим. Це має як переваги, так і недоліки для терористів.

Онлайн-платформи

Соціальні мережі та даркнет використовуються для збору коштів. Це полегшує збір коштів з різних джерел.

Методи виявлення підозрілих транзакцій в кіберпросторі

1 **Моніторинг криптовалют**

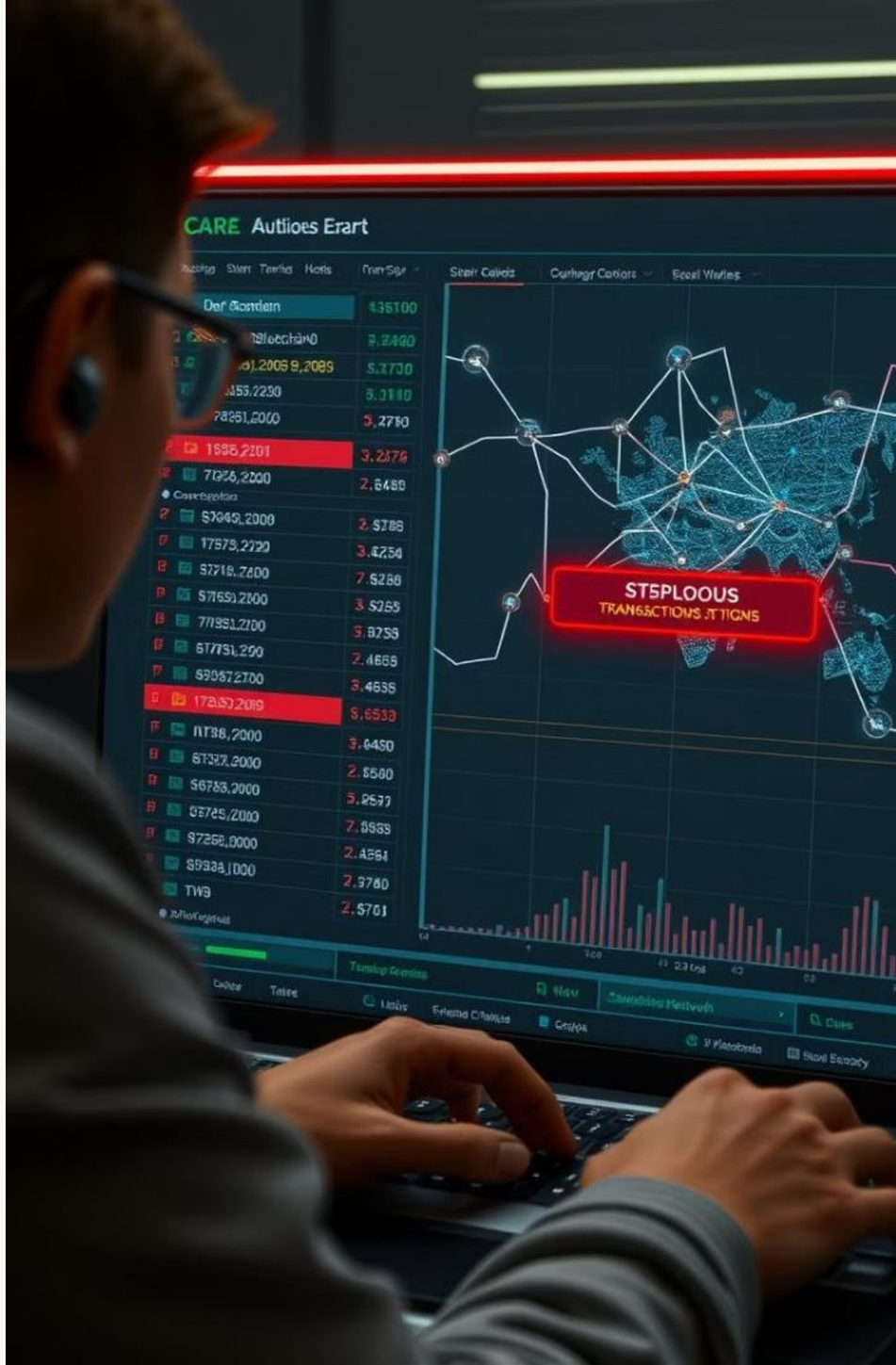
Аналіз блокчейнів та програмне забезпечення. Це дозволяє виявляти підозрілі транзакції.

2 **Онлайн-платформи**

Аналіз контенту та зв'язків між користувачами допомагає виявити підозрілу активність.

3 **Штучний інтелект**

Використовується для автоматичного виявлення аномалій. Це покращує ефективність виявлення.



Поширені схеми відмивання коштів та фінансування тероризму з використанням криптовалюти

Схема	Характеристика
Створення віртуальної юридичної особи, що приймає криптовалюту як платіжний засіб за свої послуги	Передбачає дотримання такого порядку: створення юридичної особи-фірми з можливою оплатою у криптовалюті; проведення анонімної транзакції на рахунок фірми; конвертація фірмою криптовалюти в національну валюту. Юридично гроші, що отримані з цієї підставної фірми, є повністю легальними, оскільки це оплата за послуги фірми
Використання фейкових (підроблених) електронних гаманців	Особи, купуючи товар чи послуги на популярних сервісах, перераховують гроші на фішингові гаманці, що мають інші адреси, за допомогою використання злочинцями вірусних програм
Створення фішингових сайтів (або сайтів-копій) популярних ресурсів	Нині криптовалютний фішинг тільки починає активно розвиватися. Фішингові сайти можуть бути використані для крадіжки особистої інформації, зокрема номери кредитних карток, паролі, які потім можуть бути використані для проведення незаконних фінансових операцій. Вони також можуть стати інструментом для створення фальшивих облікових записів, які потім слугуватимуть для поширення пропаганди або закликів до підтримки терористичних атак
Краудінвестінгові проєкти	Розвиток нової моделі колективного інвестування (ICO, IPO та ін.) призвело до появи шахрайських компаній, які збирають з потерпілих кошти в криптовалюті, явно не маючи на меті займатися підприємницькою діяльністю
Створення інвестиційних фондів, що працюють з використанням криптовалюти	Якщо врахувати той факт, що вони створювалися на тлі високої волатильності криптовалюти та в умовах відсутності правових гарантій захисту вкладників, логічно припустити, що більше 40% їх потенційно можуть мати кримінальні цілі

Основні цифрові тренди на їх вплив на вибір інструментів боротьби з відмиванням коштів та фінансуванням тероризму

Цифровий тренд	Характеристика	Вплив на інструменти боротьби з відмиванням коштів та фінансуванням тероризму	Перешкоди
Дані стають головним джерелом конкуренто-спроможності	Дані стають активом. Збирання, опис, зберігання та опрацювання даних дають змогу отримувати цінну інформацію для використання в ділових процесах, суспільному житті, роботі держави	BigData дозволяє підвищити ефективність, точність та швидкість зібраної та наданої інформації щодо ризикових операцій	Висуваються високі вимоги до початкових даних
Розвиток сфери Інтернету речей (Internet of things, IoT, IIoT)	Розвиток мережі, що складається із взаємопов'язаних фізичних об'єктів або пристроїв, які мають вбудовані датчики та сенсори, а також програмне забезпечення, що дає можливість здійснювати взаємодію фізичних речей із комп'ютерними системами та мережами	Оперативне отримання інформації; усунення помилок	Недостатній рівень розвитку технічного забезпечення
Цифровізація або цифрові трансформації бізнесу та галузей економіки	Цифрові технології стали базою для створення нових продуктів, цінностей, властивостей та, відповідно, основою отримання конкурентних переваг на більшості ринків	Залежно від галузі економіки, на яку здійснюється вплив, наслідки варіюються. Однозначно, що потребує посиленої уваги перевірка операцій з використанням сучасних цифрових інструментів, зокрема криптовалюти	Часта невідповідність інструментів сучасним реаліям, в силу чого виникає ряд проблем, пов'язаних з впровадженням цифрових рішень

Міжнародне співробітництво у протидії кіберзагрозам

1

Міжнародні організації

ООН, Рада Європи, FATF розробляють стандарти та рекомендації для боротьби з кіберзагрозами.

2

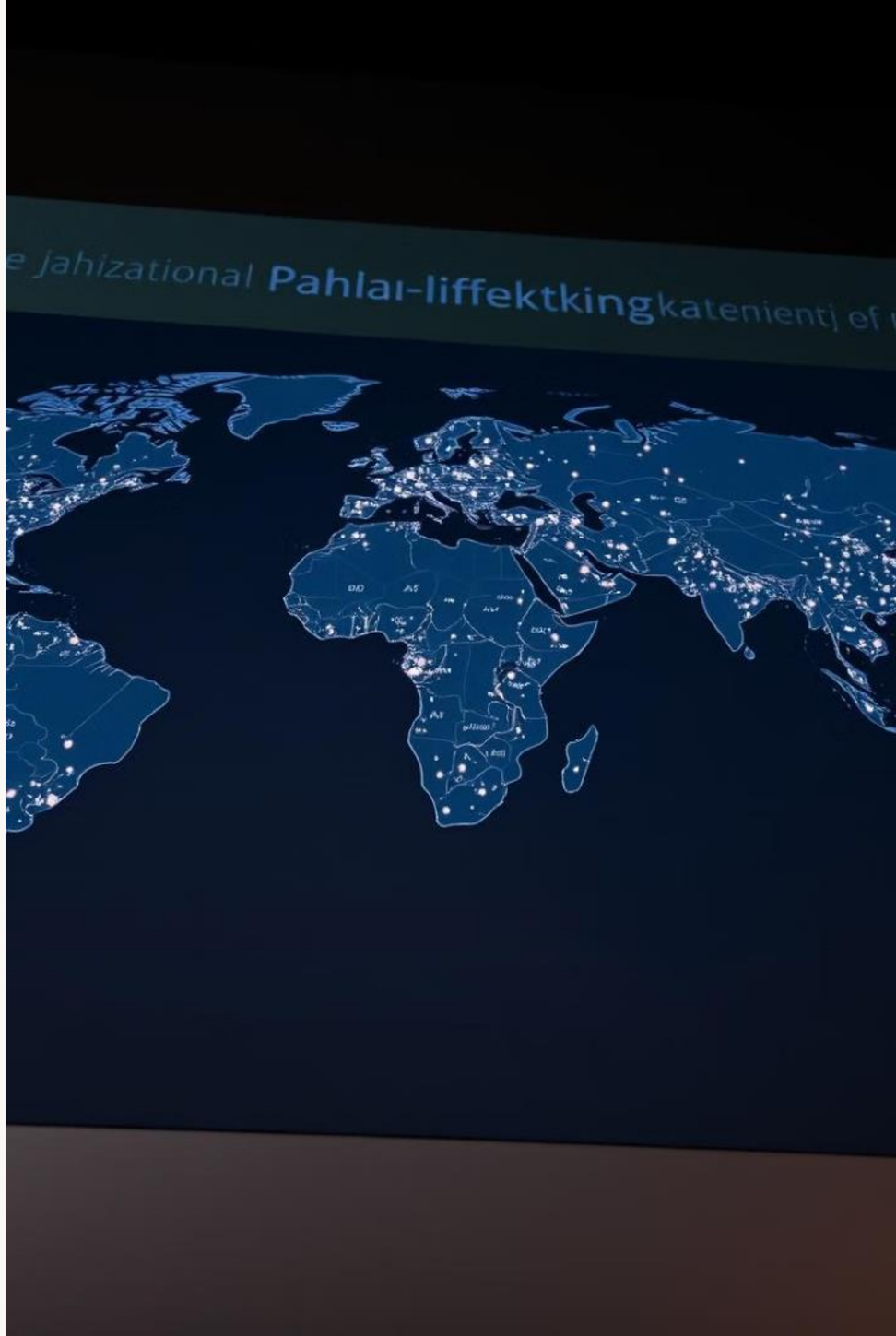
Угоди про співробітництво

Країни обмінюються інформацією та екстрадують злочинців. Це важливий аспект міжнародної співпраці.

3

Гармонізація законодавства

Важливо узгодити закони у сфері кібербезпеки та боротьби з фінансуванням тероризму.



Цифрові інструменти в системі протидії фінансуванню тероризму

Big Data Analytics

Інструменти для аналізу великих обсягів даних.

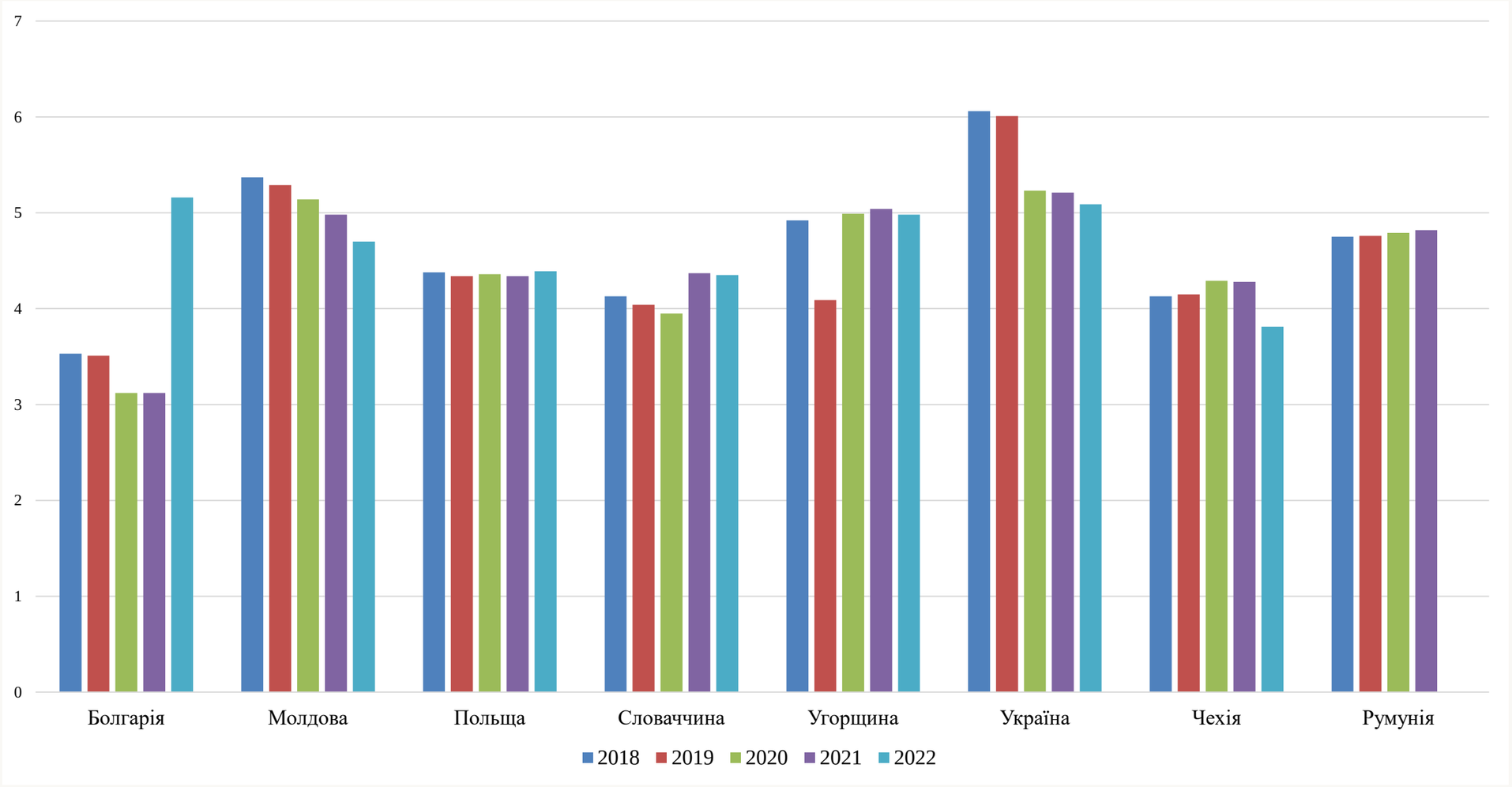
Chainalysis, CipherTrace

Програмне забезпечення для аналізу криптовалютних транзакцій.

Системи виявлення

Інструменти для захисту критичної інфраструктури від кібератак.

Значення Базельського індексу AML для країн Східної Європи за 2018-2022 рр.



Використання криптовалют для фінансування збройних конфліктів

Обхід санкцій

Криптовалюти використовуються для обходу санкцій.

Блокування транзакцій

Методи відстеження та блокування транзакцій.

Роль криптобірж

Криптобіржі повинні протидіяти цьому явищу.

Отже,...

1 кіберпростір – важливе середовище для фінансування тероризму.

2 потребує міжнародного співробітництва та цифрових інструментів.

3 необхідне постійне вдосконалення методів протидії.