Серійний номер: ДСФМУ-ДК-2024-017
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Великі технологічні компанії та цифрові гаманці

Документ "CP24/9 Big Tech and Digital Wallets: Call for Information" від Payment Systems Regulator (PSR) та Financial Conduct Authority (FCA) є закликом до надання інформації щодо впливу цифрових гаманців та великих технологічних компаній на платіжні системи у Великій Британії. Документ аналізує поточне використання цифрових гаманців, їх функціональні можливості, конкуренцію між платіжними системами та вплив на споживачів і бізнес. **Основні теми включають зручність і швидкість розрахунків, безпеку транзакцій, витрати на здійснення платежів, а також регуляторні аспекти та можливі ризики для фінансової стійкості**. PSR та FCA прагнуть зрозуміти, як цифрові гаманці можуть сприяти зростанню популярності платежів та які бар'єри можуть існувати на цьому шляху. Також розглядаються питання захисту прав споживачів і можливі майбутні загрози, пов'язані з використанням цифрових гаманців.

Ключові висновки

1. **Зростання використання цифрових гаманців:**

Більше половини дорослого населення Великої Британії використовує цифрові гаманці. Частка роздрібних платежів, здійснених через цифрові гаманці, зростає, особливо в електронній комерції.

2. **Вплив великих технологічних компаній:**

Великі технологічні компанії, такі як Apple і Google, домінують у сфері цифрових гаманців завдяки своїм екосистемам та інноваційним рішенням.

3. **Конкуренція між платіжними системами:**

Цифрові гаманці можуть сприяти зростанню популярності платежів з рахунку на рахунок, що створює конкуренцію для карткових платежів. Існують бар'єри для інтеграції таких платежів у цифрові гаманці, включаючи регуляторні вимоги та необхідність адаптації глобальних послуг під місцеві ринки.

4. **Безпека та захист прав споживачів:**

Цифрові гаманці зазвичай забезпечують високий рівень безпеки завдяки біометричній аутентифікації та токенізації. Важливо зрозуміти, як розподіляються відповідальність і ризики між різними учасниками платіжних транзакцій.

5. **Регуляторні аспекти:**

PSR та FCA досліджують, як цифрові гаманці вписуються в існуючу регуляторну рамку та які зміни можуть бути необхідними для забезпечення ефективної конкуренції та захисту прав споживачів.

6. **Майбутні перспективи:**

Вплив цифрових гаманців на платіжні системи продовжує зростати, і очікується, що нові функціональні можливості, такі як інтеграція з відкритим банкінгом, будуть стимулювати інновації та покращувати доступ споживачів до фінансових послуг.

https://psr.org.uk/media/yqinyhhn/cp24-9-cfi-digital-wallets-july-2024-v2.pdf

Оновлення найкращих практик ЄС для ефективного впровадження обмежувальних заходів

Документ є детальним посібником, виданим Генеральним секретаріатом **Ради Європейського Союзу**, щодо найкращих практик для ефективного впровадження обмежувальних заходів, відомих як санкції. Він **надає рамкові умови для ідентифікації та визначення осіб та організацій, на які поширюються цільові обмежувальні заходи, забезпечуючи узгодженість та ефективність по всьому ЄС**.

Ключові розділи включають:

- Вступ: Керівні принципи та мандати для моніторингу та оцінки обмежувальних заходів ЄС, з акцентом на розробку найкращих практик.
- Визначення та Ідентифікація: Методи ідентифікації осіб чи організацій для санкцій, вирішення питань помилкової ідентифікації та процес виключення з санкційного списку.
- Фінансові обмежувальні заходи: Законодавчі рамки, процедури заморожування активів, обсяг фінансових заходів та ролі економічних операторів і громадян.
- Заборони та координація: Правила надання товарів та важливість координації та співпраці між країнами-членами ЄС та міжнародними організаціями.

Ключові висновки:

1. **Узгодженість в ідентифікації**: Важливість використання детальних ідентифікаторів для визначених осіб або організацій, щоб уникнути проблем з помилковою ідентифікацією та забезпечити ефективність санкцій.
2. **Комплексна структура**: Документ визначає надійну законодавчу та адміністративну структуру для впровадження фінансових обмежувальних заходів, включаючи заморожування, вилучення та конфіскацію активів.
3. **Координація та обмін інформацією**: Наголошується на необхідності ефективної комунікації та координації між країнами-членами, інституціями ЄС та міжнародними організаціями для належного впровадження санкцій.
4. **Правові та гуманітарні міркування**: Під час виконання санкцій передбачено положення для забезпечення основних прав людини та гуманітарних потреб, таких як надання коштів для базових потреб та правового захисту.
5. **Відсутність відповідальності та винятки**: Забезпечує правовий захист для тих, хто виконує санкції добросовісно, та визначає обставини, за яких можуть бути надані винятки.

Ці керівні принципи мають на меті створити узгоджений і єдиний підхід до впровадження обмежувальних заходів у межах ЄС, збалансовуючи правозастосування з гуманітарними міркуваннями.

https://data.consilium.europa.eu/doc/document/ST-11623-2024-INIT/en/pdf

Проект посібника з управління та культури ризику

Європейський центральний банк (ЄЦБ) розпочав публічні консультації щодо свого нового проєкту Посібника з управління та культури ризиків.

Посібник замінює наглядовий звіт 2016 року, **роз'яснює очікування нагляду та ділиться передовою практикою внутрішнього управління в банках.** Він відображає зосередженість ЄЦБ на різноманітних та ефективних органах управління, що є наглядовим пріоритетом Єдиного наглядового механізму (SSM), і встановлює очікування нагляду щодо управління та культури ризиків підконтрольних банків.

Консультації закінчуються 16 жовтня 2024 р.

Документ охоплює різні аспекти внутрішнього управління, культури ризиків, функціонування та ефективності керівних органів банків, функцій внутрішнього контролю та структури управління ризиками. Він наголошує на важливості гармонійного поєднання цих елементів для забезпечення стабільної та стійкої банківської діяльності, а також на необхідності впровадження ефективних механізмів контролю та комунікації на всіх рівнях організації.

Ключові висновки:

1. **Важливість культури ризиків**: Культура ризиків є критичним елементом для банківської стабільності, і вона повинна бути інтегрована в усі аспекти банківської діяльності, включаючи управління, комунікацію та систему винагороди.
2. **Тон від керівництва**: Важливість "тону від керівництва" підкреслюється як ключовий фактор у формуванні правильної культури ризиків. Це включає активну роль керівництва у просуванні цінностей банку та забезпеченні їх дотримання на всіх рівнях організації.
3. **Ефективна комунікація**: Для забезпечення відкритого обговорення та викликів у процесі прийняття рішень необхідно впроваджувати культуру ефективної комунікації та різноманіття поглядів.
4. **Система стимулів**: Система винагороди та стимулів повинна бути тісно пов'язана з культурою ризиків і загальною стратегією банку. Вона повинна заохочувати бажану поведінку та обмежувати надмірне прийняття ризиків.
5. **Управління та контроль**: Внутрішні контрольні функції, такі як управління ризиками, внутрішній аудит та контроль відповідності, повинні мати чітко визначені ролі та відповідальності, а також бути незалежними та ефективними.
6. **Система управління ризиками**: Рамкова структура управління ризиками є основою для забезпечення сильної культури ризиків і повинна бути інтегрована в усі стратегічні процеси банку, включаючи планування бюджету, оцінку адекватності капіталу та ліквідності.

http://surl.li/ezpgms

ESA опублікували другий пакет політичних документів у рамках DORA

Європейські наглядові органи (ESA) опублікували другий пакет політичних продуктів у рамках Акту про цифрову операційну стійкість (DORA), що є важливим кроком у підвищенні цифрової стійкості фінансового сектору ЄС. Цей випуск включає кілька ключових документів:

1. **Регуляторні технічні стандарти (RTS):** Ці проекти встановлюють детальні вимоги та рамки, розроблені для забезпечення того, щоб фінансові установи могли витримувати, реагувати та відновлюватися після всіх типів ІКТ(інформаційно-комунікаційні технології)-збоїв та загроз. Основні напрямки включають звітність про інциденти ІКТ, управління та класифікацію.
2. **Тестування на проникнення з використанням загроз (TLPT)**: Цей документ підкреслює важливість регулярного та ретельного тестування на проникнення для фінансових установ, моделюючи реальні кібератаки для оцінки їх захисту. У ньому визначено методології, обсяг і частоту таких тестувань для забезпечення стійкості до потенційних кіберзагроз.
3. **Наглядова рамка**: Документи деталізують, як компетентні органи здійснюватимуть нагляд за дотриманням фінансовими установами DORA. Це включає встановлення наглядових рамок та ролі й обов'язки різних органів у забезпеченні відповідності стандартам.
4. **Вимоги до управління ризиками ІКТ**: Рекомендації тут зосереджені на управлінні та зменшенні ризиків ІКТ у фінансових установах. Це передбачає розробку комплексних рамок управління ризиками ІКТ, включаючи ідентифікацію, оцінку та зменшення ризиків.
5. **Звітність про інциденти:** RTS і рекомендації також надають структурований підхід до звітності про інциденти, забезпечуючи, щоб фінансові установи могли швидко та ефективно повідомляти про інциденти ІКТ відповідним органам. Це допомагає своєчасно мінімізувати потенційні впливи на фінансову систему.
6. **Управління ризиками третіх сторін**: Документи охоплюють стандарти управління ризиками, пов'язаними з постачальниками послуг третьої сторони. Це включає вимоги до належної перевірки, оцінки ризиків та постійного моніторингу послуг третіх сторін.

Випуск цих політичних продуктів у рамках DORA спрямований на зміцнення цифрової операційної стійкості фінансового сектору по всьому ЄС, забезпечуючи безпечне та стабільне фінансове середовище, здатне витримувати та відновлюватися після збоїв ІКТ.

http://surl.li/wjhgtj

Оцінка загрози організованої злочинності в Інтернеті (IOCTA)

У понеділок Європол опублікував свою оцінку загроз організованої злочинності в Інтернеті (IOCTA) за 2024 рік, аналізуючи останні загрози кіберзлочинності, з якими стикається ЄС.

Ключові ідеї включають:

- Програми-вимагачі, сексуальна експлуатація дітей та шахрайство онлайн визначені як головні загрози для ЄС, що походять як з середини ЄС, так і з-за його меж.
- Висхідний тренд використання криптовалют у різних сферах злочинності, причому біткоїн все ще є основним вибором, втім альткоїни набирають обертів.
- Зростання популярності підпільних банківських мереж, які сприяють відмиванню криптовалюти.

Що далі:

- ❖ Ключовою темою звіту є зменшення ризику використання штучного інтелекту для здійснення всіх злочинів як зараз, так і в майбутньому
- ❖ Також використання технологій зв'язку з наскрізним шифруванням має бути збалансовано з вимогами конфіденційності.
- ❖ Щодо криптовалют, Європол звертає увагу на потенційну можливість для злочинців використовувати NFT на базі Bitcoin та Bitcoin-ETF як шлях для шахрайств, що викликає занепокоєння в майбутньому.

Але, можливо, однією з найбільш тривожних тенденцій, визначених у звіті, є зниження віку правопорушників у цифрову еру. Визначення пріоритетів профілактичної діяльності матиме вирішальне значення для формування висновків у наступних ітераціях цього звіту.

https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf

Регламент (ЄС) 2023/1114 про ринки криптоактивів (MiCA). Комунікація Банку Італії

Комунікація Банку Італії стосується нового регулювання криптоактивів у Європейському Союзі, яке набуло чинності 29 червня 2023 року. Регламент MiCA встановлює гармонізовані правила для випуску, пропозиції та торгівлі криптоактивами, зокрема електронними грошовими токенами (EMTs) та токенами, прив'язаними до активів (ARTs). Ці положення наберуть чинності 30 грудня 2024 року. Документ описує новий регуляторний режим, включаючи вимоги до учасників ринку, таких як банки, фінансові установи, та постачальників послуг криптоактивів (CASPs). Також у документі згадано про наглядові функції Банку Італії та інших національних органів, пов'язаних з вимогами ПВК/ФТ та захистом прав користувачів.

Регламент MiCA: Встановлює нові правила для ринку криптоактивів у ЄС, включаючи вимоги до випуску, торгівлі та пропонування криптоактивів.

Категорії криптоактивів: Включають електронні грошові токени (EMTs), токени, прив'язані до активів (ARTs), та інші криптоактиви.

Роль національних органів: Банк Італії та Consob будуть відповідальні за нагляд і регулювання ринку криптоактивів, включаючи контроль за ПВК/ФТ.

Ризики криптоактивів: Підкреслюється важливість розуміння ризиків, пов'язаних з різними типами криптоактивів, особливо у контексті їх використання як засобу платежу.

Нагляд за ринком: Зазначено важливість належного управління ризиками та дотримання регуляторних вимог для забезпечення надійності платіжних систем та захисту користувачів.

Перехідний період: Поточні постачальники послуг зобов'язані дотримуватися чинних вимог ПВК/ФТ під час переходу до нового регулювання.

http://surl.li/rganaz

Необрокери в ЄС: розвиток, переваги та ризики

Документ "Neo-brokers in the EU: Developments, benefits and risks" аналізує швидкий ріст і вплив нео-брокерів у Європейському Союзі. **Нео-брокери - це нове покоління фінансових установ, які пропонують інноваційні, онлайн-сервіси для інвестування та торгівлі, орієнтовані переважно на роздрібних клієнтів**. Основні риси їх діяльності включають доступність через мобільні додатки та веб-сайти, часто з низькими комісіями. Документ обговорює **переваги**, які нео-брокери приносять інвесторам та ринкам, зокрема **сприяючи залученню домогосподарств до ринків капіталу та зниженню транзакційних витрат**. Водночас, **нео-брокери можуть нести ризики**, пов'язані з торгівлею складними продуктами, які можуть бути невідповідними для роздрібних клієнтів, а також з використанням соціальних мереж, що може **сприяти імпульсивній торгівлі.** Документ також висвітлює регуляторні виклики, пов'язані з діяльністю нео-брокерів, та необхідність подальшого моніторингу їх впливу на ринки ЄС.

Ключові висновки

1. **Швидке зростання та вплив на ринки:** Нео-брокери зросли у своїй популярності завдяки інноваційним онлайн-платформам, що забезпечують легкий доступ до інвестиційних продуктів, особливо серед роздрібних інвесторів. Їхня діяльність сприяла зростанню участі домогосподарств у ринках капіталу.
2. **Переваги для інвесторів:** Нео-брокери пропонують зручні та доступні інвестиційні послуги, які можуть знизити транзакційні витрати та сприяти більш активній участі домогосподарств у ринках капіталу. Вони також сприяють підвищенню фінансової грамотності серед нових та молодих інвесторів.
3. **Ризики для споживачів:** Висока доступність нео-брокерів може призводити до того, що споживачі не завжди повністю розуміють, що вони купують, або торгують імпульсивно. Це особливо актуально для складних та ризикових фінансових продуктів, таких як криптовалюти та деривативи.
4. **Виклики регулювання:** Документ підкреслює необхідність посилення регулювання діяльності нео-брокерів для забезпечення захисту інвесторів та стабільності ринків. Це включає вимоги до прозорості, обов'язковість дотримання правил ринкової поведінки та попередження маніпуляцій цінними паперами.
5. **Вплив соціальних мереж:** Інтеграція функцій соціальних мереж у торгові платформи може сприяти "груповому інвестуванню" та маніпуляціям ринком. Це підвищує ризики для роздрібних інвесторів, які можуть піддаватися впливу дезінформації та приймати необґрунтовані інвестиційні рішення.
6. **Потреба в подальшому моніторингу:** Документ наголошує на необхідності продовження моніторингу розвитку ринку нео-брокерів на рівні ESMA для забезпечення ефективного нагляду та регулювання їх діяльності.

Документ надає детальний огляд поточних тенденцій, ризиків та переваг, пов'язаних з нео-брокерами в ЄС, підкреслюючи важливість збалансованого підходу до регулювання для забезпечення стабільності ринків та захисту інтересів інвесторів.

http://surl.li/rzlahg

РЕГУЛЮВАННЯ

Законопроект про постачальників послуг віртуальних активів на Сейшельських островах

Сейшельські острови роблять крок, щоб забезпечити безпечний і процвітаючий ринок віртуальних активів. Законопроект про постачальників послуг віртуальних активів 2024 року (законопроект № 12 від 2024 року) (далі - законопроект VASP), який незабаром має набути чинності, встановлює міцну законодавчу базу, розроблену для регулювання діяльності постачальників послуг віртуальних активів (VASP) і пом'якшення потенційних фінансових злочинів, такі як відмивання коштів і фінансування тероризму.

ПІДХІД СЕЙШЕЛЬСЬКИХ ОСТРОВІВ ДО РИЗИКІВ ФІНАНСОВИХ ЗЛОЧИНІВ

Після національної оцінки ризиків 2021 року, яка підкреслила значну вразливість до ризиків ВК/ФТ, пов'язаних з віртуальними активами, Сейшельські Острови визнали невідкладність впровадження суворих регуляторних заходів.

ОСНОВНІ ОСОБЛИВОСТІ СЕЙШЕЛЬСЬКОГО ЗАКОНОПРОЕКТУ VASP

Законопроект VASP вводить кілька важливих заходів, спрямованих на створення безпечного та прозорого середовища для віртуальних активів.

Ось ключові особливості:

1. **Режим ліцензування**: Законопроект VASP передбачає обов'язкову систему ліцензування для конкретних продуктів і послуг віртуальних активів, включаючи постачальників гаманців, біржі, постачальників брокерських та інвестиційних послуг. Це гарантує, що лише уповноважені організації можуть працювати як VASP на Сейшельських островах або з їх території, забезпечуючи захист від несанкціонованої діяльності.
2. **Критерії ліцензування**: Законопроект VASP визначає певні ключові критерії ліцензування для VASP, включаючи вимоги до капіталу, платоспроможності та страхування, заходи кібербезпеки, пруденційні вимоги, вимоги до ринкової поведінки, вимоги до аудиту та оцінку придатності та належності директорів і керівників.
3. **Реєстрація промоутерів**: промоутери первинного розміщення монет (ICO) і невзаємозамінних токенів (NFT) повинні зареєструватися, забезпечуючи прозорість і підзвітність у цих інноваційних фінансових секторах.
4. **Заборона несанкціонованої діяльності**: Законопроект VASP забороняє рекламу або надання продуктів і послуг віртуальних активів без належного дозволу, тим самим запобігаючи шахрайству та зловживанням. Законопроект VASP також забороняє використання майнінгових установок, послуг міксерів або тумблерів і послуг валідаторів на Сейшельських островах або з їх території.
5. **Посилений моніторинг**: Законопроект VASP передбачає посилений нагляд за допомогою перевірок на відповідність та розслідувань, а дії проти онлайн-провайдерів VASP, які стверджують, що вони регулюються на Сейшельських островах, захистять споживачів і цілісність ринку.
6. **Заходи нагляду**: були запроваджені спеціальні заходи контролю для моніторингу та пом'якшення ризиків ВК/ФТ та інших ризиків фінансових злочинів, щоб гарантувати, що VASP дотримуються високих стандартів доброчесності.

РОЗШИРЕННЯ ПОВНОВАЖЕНЬ УПРАВЛІННЯ ФІНАНСОВИХ ПОСЛУГ

Управління фінансових послуг (FSA) призначено регуляторним органом, відповідальним за правозастосування законодавства VASP. FSA отримало повноваження:

- Перевіряти та розслідувати випадки невідповідності;
- Видавати та анулювати ліцензії;
- Реєстрація промоутерів ICO та NFT;
- Видавати керівні настанови та директиви для забезпечення відповідності;
- Запитувати інформацію;
- Вживати правозастосовні заходи.

Цей проактивний підхід дає FSA можливість підтримувати цілісність фінансового ландшафту Сейшельських островів.

ЗАХИСТ СПОЖИВАЧІВ ТА ОСВІТА

Важливим аспектом законопроекту VASP є його зосередженість на захисті та освіті споживачів. Підвищуючи обізнаність про шахрайство та зловживання віртуальними активами, законопроект VASP допомагає захистити споживачів від незаконної діяльності. Він вимагає достатнього захисту для жертв такої діяльності та сприяє відповідальним інноваціям і використанню технологій у просторі віртуальних активів.

ВИСНОВОК

Законопроект про постачальників послуг віртуальних активів 2024 року знаменує собою важливу віху на шляху Сейшельських Островів до безпечної, прозорої та сприятливої для інновацій екосистеми віртуальних активів. Запроваджуючи комплексні регулятивні заходи, законопроект VASP не лише усуває поточні ризики фінансових злочинів, але й закладає основу для сталого зростання та довіри споживачів до сфери віртуальних активів, що розвивається.

http://surl.li/sqmbnq

Світове законодавство та політика управління штучним інтелектом

Документ "Global AI Governance Law and Policy Series" аналізує **сучасні підходи до регулювання та політики в галузі штучного інтелекту (ШІ)** в п'яти основних юрисдикціях: Канаді, ЄС, Сінгапурі, Великобританії та США. Він надає **огляд законодавчих та політичних заходів, що вживаються для забезпечення відповідального використання ШІ, а також висвітлює історичні та контекстуальні аспекти розвитку цих підходів**. У кожній з розглянутих країн аналізуються ключові нормативні акти, ініціативи та стратегічні плани, спрямовані на впровадження безпечних і етичних систем ШІ.

Ключові висновки з документа

1. Різні підходи до регулювання ШІ:

- Канада впроваджує багаторівневу стратегію, що включає комерціалізацію досліджень, розробку стандартів та розвиток талантів.
- ЄС прийняв комплексний підхід, зокрема через AI Act (див. наступний допис), що регулює ШІ системи на основі рівня ризику.
- Сінгапур застосовує секторальний підхід без спеціалізованого регулятора для ШІ, впроваджуючи принципи відповідального використання через галузеві стандарти та добровільні рамки.
- Великобританія та США також використовують різноманітні регуляторні інструменти, від галузевих ініціатив до національних стратегій.

2. Інтеграція етичних принципів: Всі юрисдикції приділяють значну увагу етичним аспектам використання ШІ, включаючи питання прозорості, відповідальності та запобігання дискримінації.

3. **Співпраця на міжнародному рівні:** Юрисдикції активно співпрацюють у розробці міжнародних стандартів і кращих практик для ШІ, як, наприклад, у випадку з Глобальним партнерством з питань ШІ.

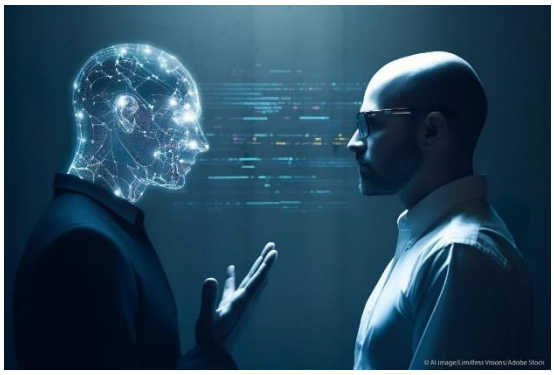
4. **Регулювання високоризикових систем:** Різні країни вводять спеціальні вимоги для високоризикових систем ШІ, таких як системи, що використовуються в охороні здоров'я, правосудді та національній безпеці.

5. **Гнучкість та адаптивність регуляторних підходів:** Усі юрисдикції визнають необхідність гнучких регуляторних механізмів, які можуть адаптуватися до швидко змінюваних технологій і нових викликів, що виникають з розвитком ШІ.

Цей документ слугує важливим джерелом інформації для розуміння поточних та майбутніх тенденцій у глобальному регулюванні штучного інтелекту, пропонуючи інсайти щодо різноманітних підходів та практик у ключових світових ринках.

https://iapp.org/media/pdf/resource_center/global_ai_governance_law_policy_series.pdf

AI Act: Короткий огляд щодо вимог, а також до кого, коли та як вони застосовуватимуться



Документ "AI Act - A brief guideline" містить **узагальнення ключових вимог та положень остаточної версії Закону про штучний інтелект ЄС** (AI Act), який був затверджений Європейським парламентом і Радою ЄС. Закон визначає широке поняття систем штучного інтелекту (ШІ) і встановлює юридичну рамку для їх регулювання, зокрема **класифікує системи ШІ за рівнем ризику на низькоризикові та високоризикові**. Високоризикові системи підлягають суворим вимогам щодо управління ризиками, прозорості, точності, надійності, кібербезпеки та людського контролю. Заборонені системи ШІ включають ті, що маніпулюють поведінкою людей, використовують біометричні дані без згоди або впроваджують соціальні кредити. Закон також передбачає зобов'язання для різних учасників ринку, таких як постачальники, імпортери та дистриб'ютори ШІ систем. Впроваджено систему санкцій за порушення положень закону, з акцентом на баланс між регулюванням ШІ та стимулюванням його розвитку.

Ключові висновки

1. **Широке визначення ШІ систем**: Законодавство ЄС надає дуже широке визначення системам штучного інтелекту, охоплюючи всі системи, які діють автономно, адаптуються і навчаються на основі отриманих даних.
2. **Двоїстий режим регулювання ризиків:** AI Act розділяє ШІ системи на низькоризикові та високоризикові, встановлюючи різні вимоги до кожної категорії. Високоризикові системи мають суворіші регуляторні вимоги.
3. **Управління ризиками та прозорість:** Високоризикові ШІ системи повинні мати систему управління ризиками, бути прозорими та забезпечувати точність, надійність і кібербезпеку. Вони також повинні бути розроблені так, щоб їхні рішення могли бути пояснені користувачам.
4. **Заборона певних систем ШІ:** AI Act забороняє системи ШІ, що маніпулюють поведінкою людей, використовують біометричні дані без згоди або реалізують соціальні кредити.
5. **Обов'язки постачальників та користувачів ШІ:** Закон зобов'язує постачальників, імпортерів та користувачів ШІ систем виконувати низку вимог, включаючи забезпечення

відповідності систем вимогам закону, проведення оцінок впливу на фундаментальні права та реєстрацію високоризикових систем у базі даних ЄС.

6. **Санкції та стимулювання розвитку:** Впроваджено систему санкцій, засновану на загальному обігу компаній або фіксованій сумі, залежно від того, що вище. Водночас, закон передбачає певні пом'якшення для малих і середніх підприємств, щоб не стримувати розвиток ШІ.
7. **Транскордонний вплив:** AI Act має транснаціональний вплив і застосовується до всіх учасників ринку, незалежно від того, де вони знаходяться, якщо їхні ШІ системи використовуються в ЄС.

Цей документ є важливим кроком у напрямку комплексного регулювання штучного інтелекту, що має на меті забезпечити безпеку, етичність та відповідальність у використанні ШІ технологій.

https://www.gamingtechlaw.com/wp-content/uploads/2024/07/AI-Act-A-brief-guideline-12.07.2024.pdf

Політика щодо доступу небанківських постачальників платіжних послуг до платіжних систем, керованих центральним банком, і до рахунків центрального банку

📣📝 19 липня 2024 р. Європейський центральний банк (ЄЦБ) випустив прес-реліз, у якому повідомляє, що **Євросистема визначила узгоджену політику, яка дозволяє небанківським постачальникам платіжних послуг (PSP) отримувати доступ до керованих центральним банком платіжних систем**, включаючи TARGET. Небанківські PSP включають платіжні установи (PI) та установи електронних грошей (EMI).

Ключові моменти політики:

▶ Починаючи з квітня 2025 року, небанківські постачальники послуг, які відповідають певним вимогам, матимуть доступ до TARGET, включаючи T2 (для здійснення платежів) і TIPS (для здійснення миттєвих платежів).

▶ Вимоги будуть викладені в Керівництві TARGET і будуть такими самими, як і ті, які зараз застосовуються до кредитних установ.

▶ Володіння рахунком у платіжній системі центрального банку має на меті дати можливість небанківським постачальникам розмістити кошти для виконання своїх розрахункових зобов'язань за поточний робочий день.

▶ Національні центральні банки в єврозоні створять умови для доступу небанківських постачальників послуг до національних платіжних систем відповідно до політики Євросистеми.

▶ Регулювання миттєвих платежів дозволяє небанківським постачальникам платіжних послуг зберігати кошти на рахунках центрального банку, якщо це дозволено.

✅ Постачальники послуг, які планують отримати доступ до TARGET, повинні стежити за оновленими правилами TARGET і узгодити свої внутрішні процеси.

http://surl.li/cdqpbu

САНКЦІЇ

Санкції за порушення прав людини

ЄС ухвалив нові санкції за порушення прав людини

Рада затвердила додаткові санкції проти фізичних та юридичних осіб, відповідальних за серйозні порушення прав людини в усьому світі, включаючи тортури та систематичне та широко поширене сексуальне та гендерне насильство. Рішення було прийнято в рамках глобального режиму санкцій ЄС щодо прав людини.

Серед осіб, які потрапили під санкції:

- Абдель Карім Мохаммад Ібрагім, начальник штабу сирійської армії, і Алі Махмуд Аббас, колишній міністр оборони Сирії та заступник головнокомандувача сирійської армії
- Рі Чанг Де, міністр державної безпеки Корейської Народно-Демократичної Республіки
- Євген Соболєв, керівник так званої «пенітенціарної служби», встановленої Москвою на тимчасово окупованій Херсонщині в Україні.

http://surl.li/dhpsdv

Виявлення п’яти найпоширеніших методів ухилення від санкцій

Документ "Detecting Five Common Sanctions Evasion Techniques" від TRM Labs надає огляд п’яти основних методів обходу санкцій, які використовують злочинці у криптоактивах, і пропонує стратегії для виявлення та протидії цим методам. Документ включає **аналіз сучасного стану санкційної політики, вимоги до дотримання санкцій для криптоактивів та майбутні кроки для вдосконалення програм санкційного контролю** з використанням блокчейн-аналітики.

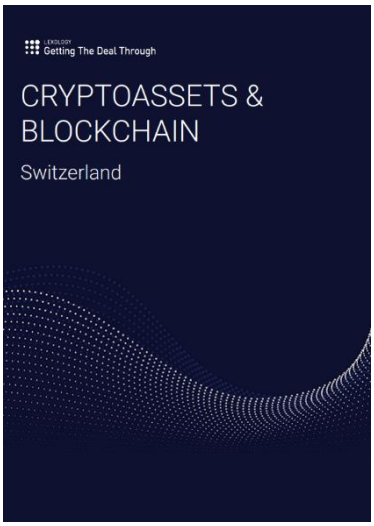
1. **Зміна адрес**: Злочинці створюють нові криптоадреси для уникнення санкцій, що вимагає частого і ретельного скринінгу адрес.
2. **Зміна імен**: Підсанкційні суб'єкти змінюють юридичні імена, щоб уникнути виявлення, що потребує ретроспективного скринінгу та використання розвідки загроз.
3. **Обхідні транзакційні схеми**: Використання складних схем транзакцій, таких як міксери та кросс-чейн свопи, для приховування слідів.
4. **Використання посередників**: Злочинці використовують третіх осіб або установи в країнах з менш суворими законами для обхідних операцій.
5. **Приховування місцезнаходження**: Використання VPN і проксі-серверів для маскування реального місцезнаходження та уникнення санкційного контролю.

Цей документ допомагає криптокомпаніям зрозуміти та впроваджувати ефективні методи боротьби з обходом санкцій, що є важливим для забезпечення фінансової безпеки і дотримання міжнародних стандартів.

http://surl.li/dzxvzy

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

КРИПТОАКТИВИ ТА БЛОКЧЕЙН: ШВЕЙЦАРІЯ



Швейцарія продовжує лідирувати в регулюванні крипторинку завдяки своїй принциповій та технологічно нейтральній законодавчій базі. Основні моменти з останнього звіту:

1. **Нормативно-правова база**: не існує спеціальних законів про криптовалюту; натомість застосовуються чинні правила фінансового ринку. Управління з нагляду за фінансовим ринком Швейцарії (FINMA) класифікує криптоактиви на три типи: платіжні токени, токени корисності та токени активів.

2. **Державна політика**: Уряд Швейцарії прагне створити сприятливе середовище для фінтех- і блокчейн-компаній, одночасно борючись зі зловживаннями, такими як відмивання коштів і фінансування тероризму.

3. **Торгівля криптоактивами**: для професійної торгівлі криптоактивами, які кваліфікуються як цінні папери, потрібен дозвіл FINMA. Децентралізовані та однорангові біржі зазвичай не регулюються, якщо вони не контролюють приватні ключі або не впливають на транзакції.

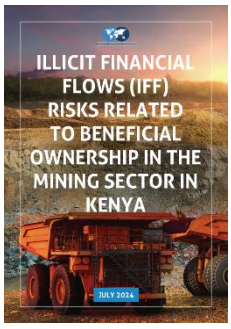
4. **Протидія відмиванню коштів (ПВК)**: закони про ПВК застосовуються до криптовалютних транзакцій, вимагаючи від фінансових посередників перевірок KYC і дотримання «Travel Rule» для платіжних токенів.

5. **Криптомайнінг**: діяльність з майнінгу не підпадає під дію фінансових правил, якщо тільки вона не передбачає стейкінг для третіх сторін, для чого може знадобитися фінтех або банківська ліцензія.

6. **Останні тенденції**: швейцарський ринок очікує отримання першої ліцензії на торговий центр DLT. Крім того, нова позиція FINMA щодо послуг стейкингу, які потребують банківських ліцензій, перебуває під пильною увагою в галузі.

https://mll-legal.com/wp-content/uploads/2024/01/Switzerland-Cryptoassets-Blockchain.pdf

Ризики незаконних фінансових потоків, пов'язані з бенефіціарним володінням у гірничодобувній галузі Кенії.



Global Financial Integrity (GFI) опублікувала звіт «Ризики незаконних фінансових потоків, пов'язані з бенефіціарною власністю у гірничодобувному секторі в Кенії». **У звіті розглядається нормативно-правова база гірничодобувної галузі Кенії, досліджуються проблеми та прогалини у впровадженні бенефіціарної власності**.

Ключові моменти звіту:

- **Нормативно-правова база**: Оцінка поточної політики та нормативних актів у гірничодобувному секторі Кенії, підкреслюючи необхідність реформ для зменшення ризиків, пов'язаних з незаконними фінансовими потоками (IFF).
- **Податки на прибуток підприємств і роялті від видобутку корисних копалин**: аналіз існуючої системи оподаткування, виявлення потенційних вразливостей і лазівок, які можуть сприяти незаконній фінансовій діяльності.
- **Проблеми в імплементації Бенефіціарної Власності**: дослідження юридичних, адміністративних та операційних труднощів, які перешкоджають прозорості бенефіціарної власності.

- **Рекомендації**: стратегічні пропозиції щодо зміцнення нормативно-правової бази, вдосконалення механізмів правозастосування та сприяння більшій прозорості у гірничодобувному секторі.

Звіт сприяє глобальній боротьбі з незаконними фінансовими потоками, зокрема у видобувних секторах. GFI продовжує працювати із зацікавленими сторонами в Кенії та за її межами, щоб сприяти фінансовій цілісності та сталому розвитку.

http://surl.li/gyfaze

Крім токенізації активів: зміна ролі обслуговування активів

📈 Інвестиційний ландшафт, що розвивається: впровадження цифрових інновацій 🌐

Інвестиційний ландшафт постійно розвивається, тепер швидше, ніж будь-коли, завдяки новим інноваціям, які глибоко змінюють екосистему. HSBC у співпраці з Northern Trust пояснює, як еволюція в обслуговуванні активів змінить ландшафт фінансових послуг.

Зростання цифрових активів та інфраструктури 🌟

Зростання цифрових активів, розвиток цифрової інфраструктури та ширшої цифрової екосистеми впливають майже на всі аспекти інвестиційної галузі.

Токенізація: ключовий каталізатор змін 💡

У цьому цифровому об’єктиві токенізація стала ключовим каталізатором змін. Це дає змогу галузі стати більш неопосередкованою та демократизованою. Це підвищує прозорість, підвищує ефективність витрат і впливає на все від торгівлі, ціноутворення та ліквідності цінних паперів до потенційно ефективнішого клірингу та розрахункових процесів.

Вплив на обслуговування активів

Токенізація разом із ширшим розвитком цифрового світу ставить під сумнів те, як працюють постачальники послуг з обслуговування активів. Це сприяє створенню середовища для більшої співпраці, оскільки компанії, які обслуговують активи, прагнуть створювати надійні рішення на майбутнє.

http://surl.li/bnjgsd

Huione Guarantee: багатомільярдний ринок, який використовують онлайн-шахраї

Дослідження від Elliptic розкриває діяльність кібер-шахрайського ринку Huione Guarantee, що активно функціонує в Південно-Східній Азії, особливо в Камбоджі. Платформа Huione Guarantee, що є частиною Huione Group, виступає як масштабний посередник у торгівлі технологіями, персональними даними та послугами з відмивання грошей. Загальний обсяг транзакцій на цій платформі перевищує 11 мільярдів доларів.

Автори розкривають механізми шахрайства, такі як схеми "pig butchering", де жертви переконуються інвестувати в фіктивні криптовалютні проекти. Важливим аспектом діяльності

Huione Guarantee є використання криптовалют, зокрема USDT, для проведення анонімних і важковідстежуваних фінансових операцій. Використання криптовалют, зокрема USDT, для здійснення та відстеження транзакцій робить процес відмивання грошей більш складним для виявлення та розслідування правоохоронними органами. Таким чином, Huione Guarantee надає широкий спектр послуг з відмивання грошей та інших інструментів для здійснення шахрайства, таких як підроблені документи та інфраструктура для приховування слідів фінансових злочинів.

Важливим фактором, який сприяє безперешкодній діяльності платформи, є її зв'язки з корумпованими посадовцями в Камбоджі. Це робить правове переслідування більш складним і дозволяє шахраям залишатися непоміченими.

Дослідження також висвітлює небезпеку, яку становить така діяльність для міжнародного фінансового порядку та підкреслює необхідність міжнародної співпраці у боротьбі з кіберзлочинністю та відмиванням грошей. Діяльність цієї платформи призвела до значного збільшення кібер-шахрайств у регіоні, що підкреслює необхідність міжнародної співпраці у боротьбі з кіберзлочинністю та відмиванням грошей, а також потребу у впровадженні більш ефективних механізмів протидії таким злочинам.

https://www.elliptic.co/blog/cyber-scam-marketplace

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Бенефіціарна власність та підтримка Глобального фонду ЄС

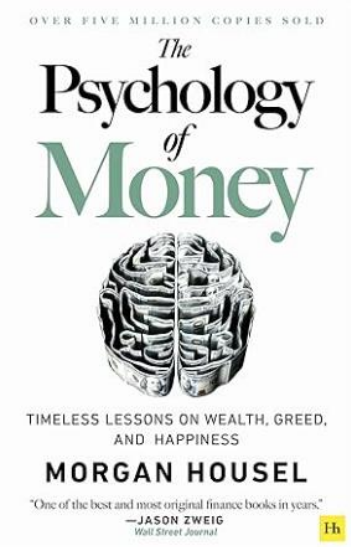
🐿 «Бенефіціарний власник» означає фізичну особу (особи), яка в кінцевому підсумку володіє або контролює клієнта, та/або фізичну особу, від імені якої здійснюється операція. Сюди також входять ті особи, які здійснюють остаточний ефективний контроль над юридичною особою чи правовим утворенням.

У цьому інтерв'ю ключовий експерт із бенефіціарної власності Глобального Фонду ЄС Александр Тайманс говорить про важливість підтримки країн у зміцненні їхніх стандартів бенефіціарної власності.

Ця підтримка допоможе їм виявити та застосувати санкції до осіб та/або компаній, які приховують або відмивають своє злочинне майно чи діяльність у підставних компаніях чи інших складних структурах, а також у трастах чи інших правових утвореннях. Ця робота ґрунтується на масштабній роботі FATF щодо підвищення прозорості бенефіціарної власності у всьому світі.

https://www.youtube.com/watch?v=mcFrtRVCvE0

Психологія грошей: позачасові уроки про багатство, жадібність і щастя



"The Psychology of Money: Timeless Lessons on Wealth, Greed, and Happiness" Моргана Хаусела досліджує, як людські емоції, поведінка та установки впливають на фінансові рішення та загальне розуміння грошей. Книга складається з 20 розділів, кожен з яких розглядає різні аспекти взаємовідносин людини з грошима, пропонуючи читачам практичні уроки та натхненні історії.

Автор починає з аналізу концепції постійного прагнення до більшого, показуючи, як важливо вміти зупинитися і сказати собі "досить". Хаусел підкреслює важливість удачі та ризику в житті кожної людини, пояснюючи, як випадкові події можуть впливати на фінансовий успіх. Він також розглядає, чому деякі фінансові принципи залишаються актуальними незалежно від часу, наголошуючи на необхідності мати довготривалу перспективу в інвестиціях та управлінні грошима.

Книга досліджує психологічні аспекти управління грошима, зокрема, як людські емоції можуть впливати на прийняття фінансових рішень. Хаусел розглядає питання, як багатство не завжди веде до щастя і як важливо розуміти власні фінансові цілі та пріоритети. Він також аналізує приклади людей, які досягли успіху або зазнали невдач, щоб показати, як різні підходи до грошей можуть впливати на життя.

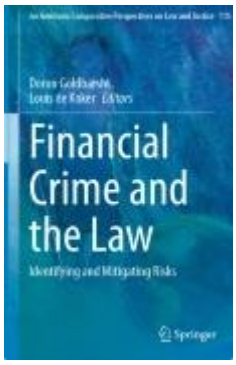
Хаусел наголошує на важливості розуміння того, що фінансовий успіх часто залежить від здатності контролювати свої емоції і приймати раціональні рішення. Він показує, як прості, але ефективні стратегії можуть допомогти досягти фінансової стабільності та щастя. Автор також підкреслює значення терпіння і довготривалої перспективи, показуючи, що успіх у фінансах часто приходить з часом і наполегливістю.

Книга завершується роздумами про те, як важливо навчатися на помилках минулого і постійно вдосконалювати свої фінансові навички. "The Psychology of Money" є цінним джерелом знань для

всіх, хто прагне краще зрозуміти взаємовідносини з грошима і знайти баланс між багатством, жадібністю та щастям.

https://www.amazon.com/Psychology-Money-Timeless-lessons-happiness/dp/0857197681

Фінансові злочини та закон: Виявлення та пом'якшення ризиків



"Financial Crime and the Law" авторства Дорона Голдбаршта є глибоким дослідженням правових аспектів фінансових злочинів, зокрема відмивання коштів та фінансування тероризму. У книзі розглядаються як міжнародні стандарти, так і національні нормативно-правові акти, які спрямовані на запобігання та боротьбу з цими видами злочинів.

Книга починається з визначення фінансових злочинів та пояснення їхнього значення для глобальної економіки. Вона досліджує історичний розвиток правових рамок та політик, що регулюють фінансові злочини, з акцентом на роботу ключових міжнародних організацій, таких як Група розробки фінансових заходів боротьби з відмиванням грошей (FATF).

Окремий розділ присвячений процесу відмивання коштів, який складається з трьох основних етапів: розміщення, розшарування та інтеграції. Голдбаршт аналізує різні методи, що використовуються злочинцями для відмивання грошей, і детально описує заходи, які застосовуються для їхнього виявлення та припинення. Він також підкреслює важливість ефективного впровадження заходів контролю у фінансових установах.

Щодо фінансування тероризму, автор відзначає його унікальні риси, що відрізняють його від інших фінансових злочинів. У книзі детально розглядаються методи виявлення і запобігання фінансуванню терористичних організацій, включаючи аналіз фінансових потоків та розробку спеціалізованих заходів моніторингу.

Далі книга досліджує різні нормативно-правові акти, які регулюють боротьбу з фінансовими злочинами, такі як Закони про банківську таємницю, Закон про протидію фінансуванню тероризму та інші ключові регуляторні документи. Голдбаршт аналізує практичні аспекти їхнього впровадження у фінансових установах і наголошує на важливості дотримання цих стандартів для забезпечення фінансової стабільності.

Особливу увагу приділено міжнародній співпраці у боротьбі з фінансовими злочинами. Автор підкреслює необхідність координації зусиль між різними країнами та організаціями для ефективної боротьби з глобальними загрозами. Він розглядає механізми та інструменти, які можуть підвищити ефективність такої співпраці, включаючи обмін інформацією та спільні розслідування.

На завершення, книга досліджує роль технологій у сприянні та боротьбі з фінансовими злочинами. Голдбаршт аналізує, як сучасні технології, такі як штучний інтелект та блокчейн, можуть бути використані для покращення заходів контролю та моніторингу. Він також обговорює виклики, пов'язані з технологічним розвитком, і необхідність постійного оновлення регуляторних рамок для адаптації до нових загроз.

"Financial Crime and the Law" є цінним ресурсом для юристів, регуляторів, дослідників та всіх, хто цікавиться питаннями фінансової безпеки та боротьби з фінансовими злочинами. Книга надає як теоретичний аналіз, так і практичні рекомендації, роблячи її корисною для широкого кола фахівців.

https://link.springer.com/chapter/10.1007/978-3-031-59543-1_1

Хакерська атака Lazarus Group на мільярд доларів: глибоке занурення в кіберзлочинність

🌟 У цьому відео розбирається одне з найскладніших кіберпограбувань в історії — злам Bangladesh Bank сумнозвісною групою Lazarus Group на мільярд доларів. Це важливо подивитися усім, хто працює в банківському секторі або зацікавлений у запобіганні фінансовим злочинам! 🌐💼

💼 Що в цій серії?

- ❖ Детальна інформація про кіберпограбування Центрального банку Бангладеш у 2016 році 🏦💻
- ❖ Ознайомлення з методами групи Lazarus та їх тривалим проникненням 🕵️‍♂️🔒
- ❖ Критична роль системи SWIFT і як її використовували 📜🔐
- ❖ Здобуті уроки та заходи запобігання майбутнім кіберзагрозам 🚨🛡️

🔍 Чому варто дивитися?

- Зрозумійте складність передових постійних загроз у кібербезпеці
- Дізнайтеся про ефективні стратегії підвищення безпеки і моніторингу
- Відкрийте для себе важливість навчання персоналу та співпраці для запобігання кіберзлочинам

https://www.youtube.com/watch?app=desktop&v=kz9srqf1n50&feature=youtu.be

Тортури та експлуатація: Внутрішній світ шахрайських ферм у Південно-Східній Азії

Дослідження ООН висвітлює проблему зростання "шахрайських ферм" у Південно-Східній Азії, які керуються міжнародними злочинними угрупованнями. Ці ферми змушують людей займатися шахрайством або практикують сексуальну експлуатацію, часто під загрозою тортур і насильства за невиконання квот.

Жертви живуть у жахливих умовах, працюючи в приміщеннях, замаскованих під легальні бізнеси, такі як онлайн-ігри та караоке-бари. Проблема посилюється через корупцію та недостатню правову базу для боротьби з такими злочинами.

ООН разом з місцевими органами влади закликає до посилення міжнародної співпраці для вирішення цієї проблеми. Ця співпраця включає посилення законодавства, обмін інформацією та координацію зусиль з різними країнами для викорінення таких злочинних схем. Важливо забезпечити захист прав людини та надати підтримку жертвам, включаючи медичну, психологічну та юридичну допомогу. ООН також підкреслює необхідність підвищення обізнаності громадськості про ці проблеми і залучення громадянського суспільства до боротьби з експлуатацією. Міжнародні організації, уряди та неурядові організації повинні об'єднати зусилля для створення ефективних стратегій протидії шахрайським фермам та забезпечення справедливості для жертв.

http://surl.li/rdcahk

Південно-Східна Азія, «нульова точка» глобальної індустрії шахрайства

Подкаст "Southeast Asia: The Ground Zero for Global Scamming Industry" від United Nations News досліджує, як Південно-Східна Азія стала центром глобальної індустрії шахрайства. Ведучі обговорюють різноманітні методи, що використовуються шахраями в регіоні, такі як "pig butchering" - схеми, де жертви переконуються інвестувати в фіктивні криптовалютні проекти. Важливим аспектом подкасту є аналіз впливу місцевої корупції на сприяння цим незаконним діям. Криптовалюти, зокрема USDT, грають ключову роль у відмиванні грошей та проведенні шахрайських операцій.

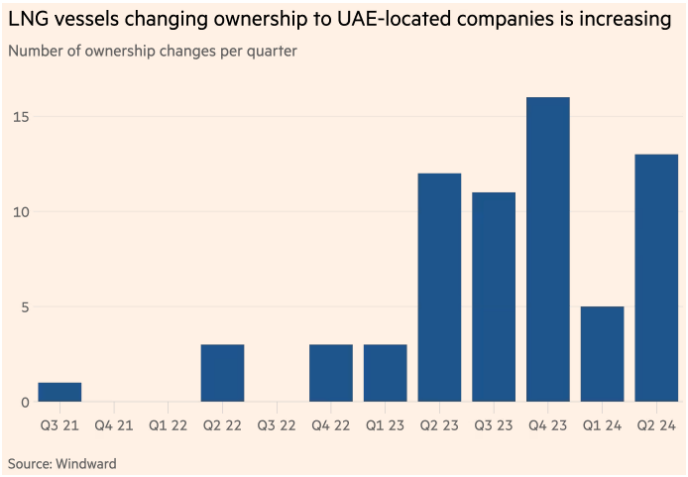
Подкаст також висвітлює важливість міжнародної співпраці у боротьбі з кіберзлочинністю. Обговорюються можливі заходи для покращення виявлення та попередження шахрайських схем, а також необхідність посилення правових та технічних заходів на глобальному рівні. Ведучі підкреслюють значення прозорості та співпраці між країнами для ефективного протистояння зростаючій загрозі кіберзлочинності.

Цей епізод надає глибокий аналіз поточної ситуації та пропонує шляхи вирішення проблеми, яка стає все більш актуальною у світовій спільноті. Для детальнішого ознайомлення ви можете прослухати подкаст за посиланням.

http://surl.li/wisrde

ІНШІ НОВИНИ

Таємничі покупці, пов’язані з Росією, накопичують «тіньовий флот» СПГ



Аналіз, проведений The Financial Times, показує, що пов’язані з Росією організації, які базуються в основному в ОАЕ, створюють тіньовий флот суден для перевезення скрапленого природного газу (СПГ) паралельно з постійно зростаючим тіньовим флотом сирої нафти та нафтопродуктовиків, які Росія почала будувати ще в 2022 році. «З другого кварталу 2023 року понад 50 суден СПГ змінили власників на компанії, розташовані в ОАЕ [...] До цього такі операції були рідкістю».

Звичайний метод полягає в тому, щоб шукати старі кораблі, від яких готові відмовитися, та викуповувати їх за завищеною ціною, перереєструвати їх у юрисдикціях, які відомі тим, що тримають під прапором судна тіньового нафтового флоту Росії, і надати їм тіньову власність, технічне управління та операційну структуру. Такі кораблі будуть брати участь у всіх видах підозрілої поведінки, перебуваючи в морі, включно з маніпуляціями AIS (спуфінг), перевантаженням товару з судна на судно на ряду з іншими тіньовими танкерами та широким документальним шахрайством.

З 2022 року СПГ підпадає під набагато менш жорсткі санкції, ніж усі інші основні російські товари. Зрозуміло, що Росія готується до посилення західних санкцій у майбутньому і намагається максимально їх випередити. В цей час російський СПГ підпадає під наступні обмеження в США, ЄС і Великобританії:

***

ІМПОРТНІ ОБМЕЖЕННЯ (також імпортне ембарго):

>> США (з 03.2022 р.). Повна заборона імпорту та супутніх послуг.

>> Великобританія (з 10.2022 р.). Повна заборона імпорту та супутніх послуг.

>> ЄС (з 06.2024 р.). Пряма та непряма закупівля, імпорт або передача СПГ, що походить із Росії або експортується з Росії через СПГ-термінали ЄС, які не підключені до об’єднаної системи природного газу ЄС, заборонені.

***

ОБМЕЖЕННЯ ПОСЛУГ:

ЄС (з 06.2024 року): Надання послуг з перевантаження в ЄС, що використовується для перевантаження СПГ, що походить із Росії або експортується з Росії, заборонено, включаючи пряму чи непряму технічну допомогу, брокерські послуги, фінансування чи фінансову допомогу.

***

НОВІ ІНВЕСТИЦІЙНІ ОБМЕЖЕННЯ:

>> США (з 04.2022 р.).

>> Великобританія (з 07.2022 р.).

>> ЄС (з 06.2024 року щодо інвестицій, необхідних для завершення проектів СПГ)

https://www.ft.com/content/f74756c8-82a5-4977-ac80-7fe6cda630ac?sharetype=blocked

Як правоохоронні органи борються зі складним схемами відмивання криптовалюти

Правоохоронні органи стикаються з проблемами у боротьбі зі складними схемами відмивання криптовалюти. Незважаючи на зниження використання крипто міксерів, таких як Tornado Cash, через агресивні репресії, злочинці адаптувалися, використовуючи кросчейн мости та протоколи децентралізованого фінансування (DeFi). Lazarus Group, північнокорейський хакерський колектив, перейшов на використання таких платформ, як YoMix, для відмивання коштів, підкреслюючи постійну адаптивність кіберзлочинців, незважаючи на регулятивний тиск.

http://surl.li/cpcjiq

Крипторегуляторні питання: положення MiCA щодо стейблкойнів стала чинною, а Circle став першим емітентом, який отримав повне схвалення

У цьому випуску Elliptic оновлення політики та нормативних питань, розглядаються деякі ключові події, пов’язані з криптовалютами в усьому світі 🌎:

- EU Положення MiCA щодо стейблкойнів стала чинною, а Circle став першим емітентом, який отримав повне схвалення
- SG Paxos отримує дозвіл на випуск стейблкойнів у Сінгапурі
- DK Данський регулятор викладає міркування щодо DeFi в контексті MiCA
- EU Європейське банківське управління видає вказівки щодо Travel Rule
- KR Південнокорейські біржі перевірять токени відповідно до нової системи лістингу
- BO Болівія скасовує заборону на криптовалюту
- BS Багамські острови вимагають, щоб банки надавали доступ до CBDC

http://surl.li/znvnsu

Новий закон Сінгапуру в чотири рази збільшує штрафи для постачальників корпоративних послуг, які порушують обов’язки щодо боротьби з відмиванням коштів

У Сінгапурі було прийнято новий закон, що значно збільшує штрафи для постачальників корпоративних послуг, які порушують обов'язки з протидії відмиванню коштів, до 100 000 SGD. Всі компанії, що надають корпоративні послуги, тепер повинні зареєструватися в ACRA. Закон також поширюється на бухгалтерські компанії, що надають послуги, визначені FATF. Призначення номінальних директорів можливе лише зареєстрованими постачальниками корпоративних послуг. Нові вимоги спрямовані на боротьбу з "сінгапурським відмиванням" та забезпечення прозорості корпоративної структури. Закон було обговорено разом з антимонопольним законом, викликавши дискусії щодо витрат для малого бізнесу та суворості вимог. Нововведення підтримано під час консультацій із зацікавленими сторонами.

http://surl.li/jajikx

Як шахрайські мережі використовують фальшиву рекламу зі знаменитостями, щоб заманити інвесторів.

Стаття від SwissInfo досліджує, як шахрайські мережі використовують фальшиві реклами з участю відомих осіб для залучення інвесторів. Шахраї створюють оманливі оголошення, використовуючи імена знаменитостей.

Знаменитості, такі як Стефан Буссер, Роджер Федерер та ін., стали жертвами неправомірного використання їхніх імен і образів у оманливих оголошеннях. Ці реклами поширюються через соціальні мережі та ведуть на фальшиві інвестиційні платформи, які обіцяють високі прибутки. Жертви, зазвичай, втрачають кошти, коли вносять початковий депозит і продовжують інвестувати більші суми на прохання шахраїв.

Фальшиві платформи часто зв'язані з Кіпром, що ускладнює повернення грошей для жертв. Розслідування швейцарського телеканалу SRF показало, що ці платформи маніпулюють клієнтами, змушуючи їх вкладати більше грошей і обіцяючи високі прибутки. Постраждалі рідко можуть повернути свої інвестиції, оскільки шахрайські компанії швидко змінюють свої назви та продовжують діяти під іншими іменами.

Журналісти виявили, що, незважаючи на численні скарги на платформу Trustpilot, шахрайські схеми продовжують функціонувати, обманюючи нових жертв. Шахраї використовують складні методи соціальної інженерії та технології для створення переконливих фальшивих оголошень і платформ, що робить їхні дії особливо небезпечними для необізнаних інвесторів.

http://surl.li/fnxlbn

Кінець санкцій проти Північної Кореї… і що буде далі

Стаття "The End of North Korean Sanctions Enforcement…and What Comes Next" від Australian Institute of International Affairs аналізує поточний стан та перспективи санкцій проти Північної Кореї після того, як Росія наклала вето на продовження роботи Панелі експертів ООН, що здійснювала моніторинг виконання санкцій.

Незважаючи на те, що санкції формально залишаються чинними, їхнє дотримання суттєво послабло через відсутність підтримки з боку Росії та Китаю. Це підриває міжнародні зусилля щодо стримування ядерних і балістичних програм КНДР.

Крім цього, стаття підкреслює, що відсутність нових санкцій з 2018 року дозволила Північній Кореї значно розширити свою діяльність з уникнення санкцій, використовуючи методи, такі як нелегальна морська передача товарів. Китай і Росія продовжують порушувати санкції, що ще більше ускладнює їхнє дотримання.

Автори розглядають потенційні шляхи виходу з ситуації, пропонуючи, наприклад, запровадження автономних санкцій з боку країн G7 або вторинних санкцій проти компаній та організацій, що співпрацюють з Північною Кореєю. Незважаючи на ці пропозиції, перспективи відновлення ефективного примусового виконання санкцій залишаються невизначеними.

Нарешті, стаття прогнозує, що Північна Корея й надалі здійснюватиме провокаційні дії, такі як випробування балістичних ракет, враховуючи поточний рівень підтримки з боку Китаю та Росії. Це створює додатковий тиск на міжнародне співтовариство для пошуку нових підходів у стримуванні агресивної політики КНДР.

http://surl.li/tnddmn

Як вирішити проблему тіньових коштів у Великій Британії?

Стаття « Як вирішити проблему тіньових коштів у Великій Британії?» висвітлює зловживання, пов’язані з товариство з обмеженою відповідальністю (ТОВ) у Великій Британії. ТОВ часто використовуються для відмивання коштів, корупції та інших злочинів завдяки своїй структурі, яка забезпечує обмежену відповідальність учасників і ускладнює ідентифікацію справжніх бенефіціарних власників. Проблема посилюється через використання корпоративних і закордонних осіб, що забезпечує анонімність. Стаття наголошує на необхідності посилення законодавства, зокрема, на внесенні змін до Закону про економічні злочини та корпоративну прозорість 2023 року, який містить численні прогалини. Рекомендується обмежити використання корпоративних осіб, підвищити прозорість щодо бенефіціарних власників і покращити наглядові заходи, щоб ефективно боротися з економічними злочинами і захистити фінансову систему. Автори наголошують, що уряду слід приділяти більше уваги цим питанням, щоб забезпечити безпеку та прозорість у фінансовому секторі.

https://www.opendemocracy.net/en/how-to-fix-dark-money-new-uk-government/

Інформаційний бюлетень EBA щодо ПВК/ФТ

🚀 Будьте в курсі останніх новин від EBA!

Дізнайтеся про останні досягнення Європейського банківського управління (EBA) в боротьбі з відмиванням коштів та фінансуванням тероризму у їхньому останньому інформаційному бюлетені. Основні моменти включають:

🔍 **Віртуальні IBAN**: У травні EBA опублікувала звіт про видачу віртуальних IBAN (vIBAN) у різних країнах ЄС. Звіт визначає характеристики vIBAN, різні випадки їх використання та проблеми, пов'язані з регулюванням і запобіганням ВК/ФТ. EBA надала рекомендації щодо вирішення цих питань.

🔒 **Управління для ARTs**: У липні EBA оголосила пріоритети нагляду за емітентами ART та EMT згідно з MiCA на 2024/2025 роки. Пріоритети включають внутрішнє управління та управління ризиками, фінансову стійкість, управління технологічними ризиками та боротьбу з фінансовими злочинами.

👥 **Керівництво EBA щодо "travel rule" для боротьби з ВК/ФТ у переказах коштів та криптоактивів**: У липні EBA видала нові керівні принципи щодо "travel rule", які визначають

інформацію, що повинна супроводжувати переказ коштів або криптоактивів, а також дії, які повинні вживати постачальники платіжних послуг для виявлення відсутньої або неповної інформації.

🌐 **Керівні принципи щодо факторів ризику**: У січні EBA розширила керівні принципи щодо факторів ризику ВК/ФТ на постачальників послуг з криптоактивами (CASPs). Керівництва описують, які фактори ризику повинні враховувати CASPs при оцінці ризиків ВК/ФТ та як вони повинні їх зменшувати. Ці керівництва зараз доступні всіма офіційними мовами ЄС.

📚 **Навчальні семінари**: У травні EBA провела дводенний семінар для 350 наглядових органів ЄС з питань ПВК/ФТ, а в липні – дводенний тренінг з криптоактивів для 430 наглядових органів ЄС. Ці заходи були спрямовані на підвищення ефективності оцінки ризиків ВК/ФТ та надання знань про нову нормативну базу криптоактивів.

https://ec.europa.eu/newsroom/eba/newsletter-archives/54835

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Зростання відмивання цифрових грошей через відеоігри та криптовалюти

Нещодавні розслідування показують, що злочинці все частіше використовують цифрові технології, такі як відеоігри та криптовалюти, для відмивання грошей. Цей перехід до цифрової сфери створює значні проблеми для правоохоронних органів у всьому світі.

Цифрові інновації у відмиванні коштів: злочинці використовують криптовалюти та онлайн-ігри, щоб приховати походження незаконних коштів, використовуючи складні методи для очищення брудних грошей, що ускладнює органам влади відстеження.

Традиційне ВК vs. цифрове ВК: Традиційно відмивання коштів включало три етапи: розміщення, розпорошення та інтеграція. Тепер ці кроки копіюються в цифровому вигляді, перетворюючи готівку у криптовалюти, використовуючи цифрові міксери та торгуючи цифровими активами, такими як NFT.

Приклади: сестри Дін керували імперією контрабанди наркотиків, конвертуючи готівку в біткоіни через брокера. Такі ігри, як Axie Infinity та Counter-Strike: Global Offensive, використовувалися для відмивання грошей через внутрішньоігрові покупки та цифрові активи.

Виклики для правоохоронних органів: швидкий розвиток технологій і глобальний характер кіберпростору ускладнюють роботу правоохоронних органів. Анонімне та менш регульоване цифрове середовище дає перевагу злочинцям.

Майбутні наслідки: експерти прогнозують зростання відмивання цифрових грошей через легкість поєднання незаконних і законних грошей в Інтернеті. Посилення міжнародної співпраці та оновлені правила дуже важливі для боротьби з цією зростаючою загрозою.

AMLR і концепція «клієнта»

Для деяких підзвітних суб'єктів AMLR детально прописує кого слід вважати клієнтом

Стаття 19(1)(a) AMLR містить інформацію про те, що підзвітні суб'єкти повинні застосовувати CDD під час встановлення ділових відносин. В статті 2(19) AMLR *діловими відносинами є ділові, професійні або комерційні відносини, які пов'язані з професійною діяльністю підзвітного суб'єкта, які встановлюються між підзвітним суб'єктом та клієнтом, в тому числі за відсутності письмової угоди, і які, як очікується, повинні бути, коли контакт налагоджено, що відповідно вимагає елемент повторення або тривалості*.

Таким чином, AMLR більш широко розглядає концепцію клієнта замість того, щоб посилатися виключно на поняття ділових відносин, хоча в статті 2 не має визначення клієнта. Стаття 19(6) AMLR, однак, описує досить детально для низки конкретних підзвітних суб'єктів, кого вони мають вважати своїми клієнтами.

Obliged entity	Customers
Professional traders in precious metals and stones and high-value goods; professional traders and intermediaries in the trade of cultural goods; storers, traders or intermediaries in the trade of cultural goods and high-value goods in free zones and customs warehouses	❖ Direct customer ❖ Supplier of goods
Notaries, lawyers and other independent legal professionals intermediating a transaction, and to the extent they are the only notary or lawyer or independent legal professional	❖ Direct customer ❖ Counterparty ('both parties to the transaction')
Real estate agents	❖ Direct customer ❖ Counterparty ('both parties to the transaction')
Payment initiation service providers when performing payment initiation services	❖ Merchants
Crowdfunding service providers and crowdfunding intermediaries	❖ Natural or legal person seeking funding through the platform ❖ Natural or legal person providing funding through the platform
Article 22(3) AMLR requires credit institutions and financial institutions to obtain information to identify and verify the identity of the natural or legal persons **using any virtual IBAN they issue**, and the associated bank or payment account.	

**Overview created by Melissa van den Broek*

Ймовірно, це призведе не лише до практичних змін, але як очікується, це також призведе до (подальших) регуляторних і контрактних дилем. 🔍

Мули ідентифікаційних даних - росіяни підживлюють шахрайство з ідентифікаційними даними, продаючи зображення та відео людей із документами, що посвідчують особу

Мули ідентифікаційних даних можуть полегшити створення грошових мулів, оскільки люди продають свої селфі та фотографії за ціною від 20 доларів. Ці селфі потім використовуються для обходу KYC перевірок на криптовалютних біржах та інших сервісах.

Журналіст Джозеф Кокс із 404 Media розповів, що підпільні фабрики продають відео людей, які повертають голови вправо та вліво, і покупці можуть вибрати портрети на свій смак всього за 30 доларів.

Компанія з кібербезпеки SentiLink повідомила 404 Media, що деякі особи подорожують до таких місць, як Сербія, і платять місцевим жителям від 5 до 20 доларів за те, щоб ті зняли селфі та відео зі своїм обличчям, які потім продаються.

У новинному сюжеті також йдеться про сайт під назвою Fotodropy Store, який пропонує зображення, пов’язані з однією людиною, за 1 390 рублів (16 доларів). На сайті є різні демографічні варіанти, що дозволяють клієнтам вибирати стать і вік моделі.

Protos також виявив колекцію зі 100 фотографій чоловіків і жінок з Іспанії, Перу та Мексики. Ця колекція продавалася за 40 доларів.

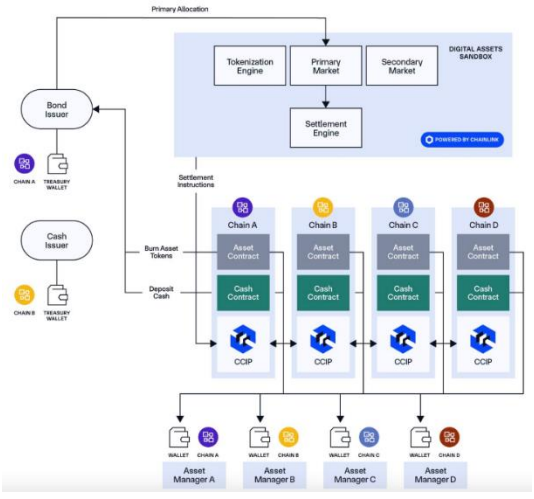
У той час як індустрія верифікації особистості прагне розробити рішення для виявлення шахрайства, проблема крадіжки особистих даних і використання «мулів» ускладнює використання верифікації особистості для відстеження таких випадків і подальшого відмивання коштів через грошових "мулів".

Ідея отримання грошей за продаж своїх біометричних даних дуже приваблива для тих, хто шукає засоби для виживання.

Не дивно, що проект WorldCoin, заснований Сэмом Альтманом, також став жертвою подібних шахрайських схем в Африці, коли скани райдужки очей багатьох африканців потрапили на чорний ринок в Китаї.

Chainlink запускає пісочницю цифрових активів для фінансових установ

Пісочниця цифрових активів (DAS) Chainlink дозволяє користувачам запускати пілотні проекти токенізації та спільне підтвердження концепції всього за кілька днів. Ця ініціатива спрямована на прискорення інновацій цифрових активів для звичайних установ.



Безпечне середовище для експериментів 🛡

«Пісочниця цифрових активів надає учасникам ринку безпечне середовище, де як фінансові установи, так і фінтех-компанії можуть експериментувати та розуміти, як технологія впливає на операційні та бізнес-моделі», — сказав Кевін Джонсон з Euroclear. «Це дає командам можливість експериментувати, вчитися та, зрештою, створювати надійні бізнес-обґрунтування для інвестування у свої стратегії цифрових активів».

Токенізація активів у реальному світі

DAS полегшує різноманітні випадки використання токенізації активів у реальному світі в пісочниці, наприклад токенізацію облігацій, заставу активів і функції торгівлі в кількох мережах.

Готові до використання бізнес-процеси

«Завдяки DAS установи можуть безперешкодно отримувати доступ до готових до використання бізнес-процесів для цифрових активів», — сказав Chainlink. «Ця платформа також дозволяє експериментувати з іншими реальними сценаріями використання цифрових активів із залученням різноманітних фінансових інструментів протягом усього життєвого циклу».