ПРІОРИТЕТИ СПІВПРАЦІ З ЄС У СФЕРІ ПРАВООХОРОННОГО СПІВРОБІТНИЦТВА, БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ, КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

Експертна підтримка впровадження порядку денного у сфері юстиції, свободи та безпеки Україна – ЄС

Громадська Синергія

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

НАЦІОНАЛЬНА ПЛАТФОРМА Форуму громадянського суспільства СХІДНОГО ПАРТНЕРСТВА

ЄВРОПА БЕЗ БАР'ЄРІВ громадська організація

Цю публікацію підготовлено експертами аналітичного центру «Європа без бар'єрів» під егідою Української Національної Платформи Форуму Громадянського суспільства Східного Партнерства за сприяння Європейського Союзу та Міжнародного фонду «Відродження» в рамках проекту «Громадська синергія».

Відповідальність за зміст документу несе аналітичний центр "Європа без бар'єрів".

Автор:
Руслан Мініч

Команда проекту:
Ірина Сушко, Руслан Мініч, Павло Кравчук

Дизайн:
Вікторія Федина

ПРІОРИТЕТИ СПІВПРАЦІ З ЄС У СФЕРІ ПРАВООХОРОННОГО СПІВРОБІТНИЦТВА, БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ, КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

Експертна підтримка впровадження порядку денного у сфері юстиції, свободи та безпеки Україна – ЄС

У рамках Ради асоціації Україна-ЄС, українська сторона розробила Новий Порядок у сфері юстиції, свободи та безпеки, що вмістив завдання за напрямками завершеного у 2017 році Плану дій з візової лібералізації з ЄС та Угоди про асоціацію, виконання якої триває.

Вона його презентувала під час саміту Україна-ЄС влітку 2018 року. У грудні під час засідання Ради асоціації Україна-ЄС його продовжили обговорювати. Рада асоціації погодилася активізувати співпрацю у сфері юстиції та внутрішніх справ.

Серед сфер взаємного інтересу відзначено протидію відмиванню коштів та фінансуванню тероризму, боротьбу з організованою злочинністю та тяжкими міжнародними злочинами. Обидві сторони підкреслили необхідність подальшої співпраці у боротьбі з кібер- та гібридними загрозами в інтересах безпеки своїх громадян.

Над цими питаннями разом з європейськими колегами, зокрема Консультаційної місії ЄС, працюють профільні міністерства та Урядовий офіс координації європейської та євроатлантичної інтеграції, який відповідає за розроблення та здійснення заходів з виконання домовленостей між Україною та Європейським Союзом.

Водночас, Новий порядок залишається не затвердженим. Варто переглянути та узгодити завдання документу в умовах нового уряду та профільних органів влади з питань європейської інтеграції.

/

1. КІБЕР-БЕЗПЕКА

Міжнародний союз електрозв'язку у 2018 році опублікував своє третє дослідження кібербезпеки у світі. Також Союз формує індекс кібербезпеки. Україна свої позиції тут щороку покращує. Зокрема, якщо у 2014 році значення індексу було 0,353, у 2017 - вже 0,501, то у 2018 - воно зросло до 0,661.

Водночас, варто відзначити, значно вищі показники держави-агресора Росії - 0,836 у 2018 році. А до першої десятки найбільш захищених країн входять Велика Британія, США, Франція, Литва, Естонія, Сінгапур, Малайзія, Канада та Норвегія.

Для посилення кібербезпеки Україна прийняла Стратегію кібербезпеки 15 березня 2016 року. **Проте останній прийнятий План заходів з її реалізації стосувався 2018 року.** Водночас, у липні 2018 року прийнято закон «Про основні засади забезпечення кібербезпеки України». Він, зокрема, вводить в українське законодавство нові важливі терміни, поняття критичної інфраструктури, а також державно-приватне партнерство. Він також визначає основних суб'єктів національної системи кібербезпеки та їхні повноваження: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Проте одного закону недостатньо. **Для його реалізації потрібні інші закони та підзаконні акти.** Водночас, варто більш чітко прописати, як державні органи мають реалізовувати свої повноваження, щоб уникнути ситуації, коли кілька органів відповідають за одне й те ж.

Тим часом, у листопаді 2018 року в Європейському Союзі набула чинності Директива щодо мережевої та інформаційної безпеки (директива NIS - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union). Її мета - посилити кібербезпеку на європейських теренах. Хоча ця директива не є обов'язковою для України, **її впровадження в українське законодавство може суттєво посилити кібербезпеку й відповідатиме євроінтеграційним прагненням країни.**

Серед іншого, вона вимагає прийняти національну стратегію безпеки мережевих та інформаційних систем, а також визначити державні інституції, які відповідають за кібербезпеку, єдину точку контакту та Групу реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT або CERT). Ці пункти Україна виконала. Щодо останнього таким органом є Команда реагування на комп'ютерні надзвичайні події України (Computer Emergency Response Team of Ukraine, CERT-UA). Це - спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

Відповідно до директиви NIS Україна має визначити обов'язкові вимоги до операторів суттєвих послуг (критичної інфраструктури) і для провайдерів цифрових послуг. Постановою Кабінету Міністрів України № 518 від 19 червня 2019 року "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" визначено, що **"власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури".**

Об'єкти критичної інфраструктури можуть бути як державної, так і приватної форми власності. Проте допоки не визначено, **які саме об'єкти вважати критичною інфраструктурою та процедуру їх аудиту, ця норма не працює. Відповідно варто виправити ці прогалини або на рівні закону, або на рівні підзаконних актів.**

Окрім того, незрозуміло, **яким чином буде визначено зобов'язання провайдерів цифрових послуг.** Такими провайдерами є онлайн ринки, пошукові системи та послуги хмарних обчислень. Директива NIS вимагає зобов'язати таких провайдерів впровадити відповідні та пропорційні технічні та організаційні міри безпеки, але на відміну від об'єктів операторів суттєвих послуг, регулятор не має здійснювати постійний нагляд та контроль за провайдерами цифрових послуг. Він реагує лише в разі наявності фактів, що провайдер цифрових послуг не відповідає вимогам директиви NIS, особливо у разі виникнення інциденту.

Ще одна новація закону про кібербезпеку – **державно-приватна взаємодія.** Тут прописані шляхи такої взаємодії, проте для практичної реалізації не вистачає чіткого механізму. Водночас, держава має продумати та пояснювати приватним підприємствам, у чому їхня користь від такої співпраці.

Водночас, відповідно до Плану заходів з реалізації Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року Україна має **укласти меморандуми про співпрацю з Європейським агентством з питань мережевої та інформаційної безпеки "ENISA", Трастовим фондом НАТО з кібербезпеки, Південно-Східним Європейським правоохоронним центром (SELEC).**

Серед міжнародних зобов'язань Україна ратифікувала Конвенцію про кіберзлочинність Ради Європи (CETS № 185) - Будапештську конвенцію. Вона виконала більшість її матеріальних положень по суті, окрім кількох важливих процедурних елементів. Зокрема, **варто внести до Кримінально-процесуального кодексу визначення поняття електронних доказів та процедуру їх збору.** Тоді українські кримінальні суди зможуть приймати файли та електронні сліди як докази. Правоохоронним органам не треба буде вилучати обладнання як доказ, достатньо буде копії. Наразі неналежне оформлення електронних доказів нерідко є підставою для їх відхилення судом.

У 2019 році Європейський Союз прийняв The EU Cybersecurity Act. Серед іншого, він визначає **нову схему сертифікації продуктів, процесів та послуг ІСТ.** Таку сертифікацію потрібно буде проходити лише один раз. Сертифікати будуть визнані на теренах всього Євросоюзу. Беручи за приклад кращі практики ЄС, **Україна може впровадити схожу систему в себе.**

Окрім законодавчих новацій, слабким елементом української кібербезпеки є **обмеженість держави у можливості забезпечити конкурентну оплату праці для залучення фахівців із кібербезпеки.**

Водночас, міжнародні партнери України, зокрема Консультативна місія ЄС, провела амбітну програму тренінгів для Міністерства внутрішніх справ та підзвітних йому відомств, щоб підвищити рівень знань тих фахівців, які задіяні в управління ІКТ та відповідають за прийняття рішень та планування.

/

2. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

У 2018 році Євросоюз посилив систему захисту персональних даних. Тоді після дворічного перехідного періоду почав застосовуватись Загальний регламент ЄС про захист даних (Regulation (EU) 2016/679, General Data Protection Regulation - GDPR).

Україна не має зобов'язання впроваджувати нові європейські правила, оскільки Угода про асоціацію та інші ключові документи підписувались ще до створення GDPR. А стаття 15 Угоди про асоціацію досить загальна і вимагає "забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів". Проте українська влада сама вирішила впровадити цей регламент і визначила відповідне завдання у Плані заходів з виконання Угоди про асоціацію, а саме: **"удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679".**

Таким чином, Україна створила координаційну робочу групу з розроблення законопроекту щодо внесення змін до Закону України "Про захист персональних даних" відповідно до положень GDPR. До неї входять та беруть активну участь у розробці відповідного законопроекту європейські експерти проекту ЄС Twinning № UA/47b "Впровадження кращого європейського досвіду з метою посилення інституційного потенціалу Секретаріату Уповноваженого Верховної Ради України з прав людини для захисту прав і свобод людини".

Наразі Уповноважений та суди є єдиними інституціями, які здійснюють контроль за додержанням законодавства про захист персональних даних. Проте цього недостатньо. GDPR вимагає створення **спеціального незалежного наглядового органу із захисту персональних даних.**

Персональні дані - це дані, які дозволяють ідентифікувати особу. Це можу бути ім'я, адреса, або навіть IP адреса. Водночас, Регламент визначає категорію **чутливих персональних даних,** захист яких має забезпечуватись більш ретельно. Це такі дані як участь у профспілках, релігійні та політичні погляди, раса та сексуальна орієнтація.

Відповідно до GDPR компанія має отримати **чітку згоду на обробку даних.** У повідомленні про збір даних має бути пояснення необхідності надати такі дані та що компанія робитиме з ними. Таке пояснення має бути письмовим та легко зрозумілим, щоб людина чітко усвідомлювала, на що вона дає згоду. Окрім того, така згода має бути надана ствердними діями користувача, а не за замовчуванням. Наприклад, він чи вона мають самі поставити "галочку" про згоду.

Компанії зобов'язані провести організаційно-технічні заходи для захисту персональних даних. Це означає, що вони повинні мати документи, у яких пояснено які дані та навіщо вони збирають, а також як довго зберігають. Призначити особу відповідальну за захист персональних даних (**data protection officer - DPO**). А також забезпечити **безпеку** персональних даних (шифрування, псевдонімізація тощо).

Водночас, GDPR дає користувачам більше контролю над персональними даними. Вони можуть надіслати компанії запит щодо інформації про їхні дані, якими та володіє. Регламент також надає право **"стирання" даних**, якщо у них немає необхідності, користувач відкликає згоду на їх обробку, відсутній легітимний інтерес, або їх обробку здійснено незаконно.

Важливим елементом GDPR є також повноваження регулятора **штрафувати** компанії за порушення положень Регламенту. Якщо компанія не належним чином обробляє персональні дані, її штрафують. Якщо немає особи відповідальної за персональні дані, штраф. Якщо порушено безпеку, штраф. Наприклад, у Польщі регулятор наклав на брокера даних штраф у розмірі 220 тисяч євро за те, що той не поінформував користувачів, що їхні дані обробляються.

А Франція оштрафувала Google на 50 мільйонів євро за те, що він недостатньо "чітко та зрозуміло" інформував користувачів про те, як їхні дані будуть використовуватись. Також в угоді з користувачем пташку у віконці, що дозволяє використання даних, було поставлено заздалегідь. А регламент вимагає, щоб користувач сам її поставив.

Водночас, варто відзначити, що регулятори країн ЄС все ж віддають перевагу діалогу перед санкціями, особливо з малими операторами, де обробка персональних даних не є основною діяльністю.

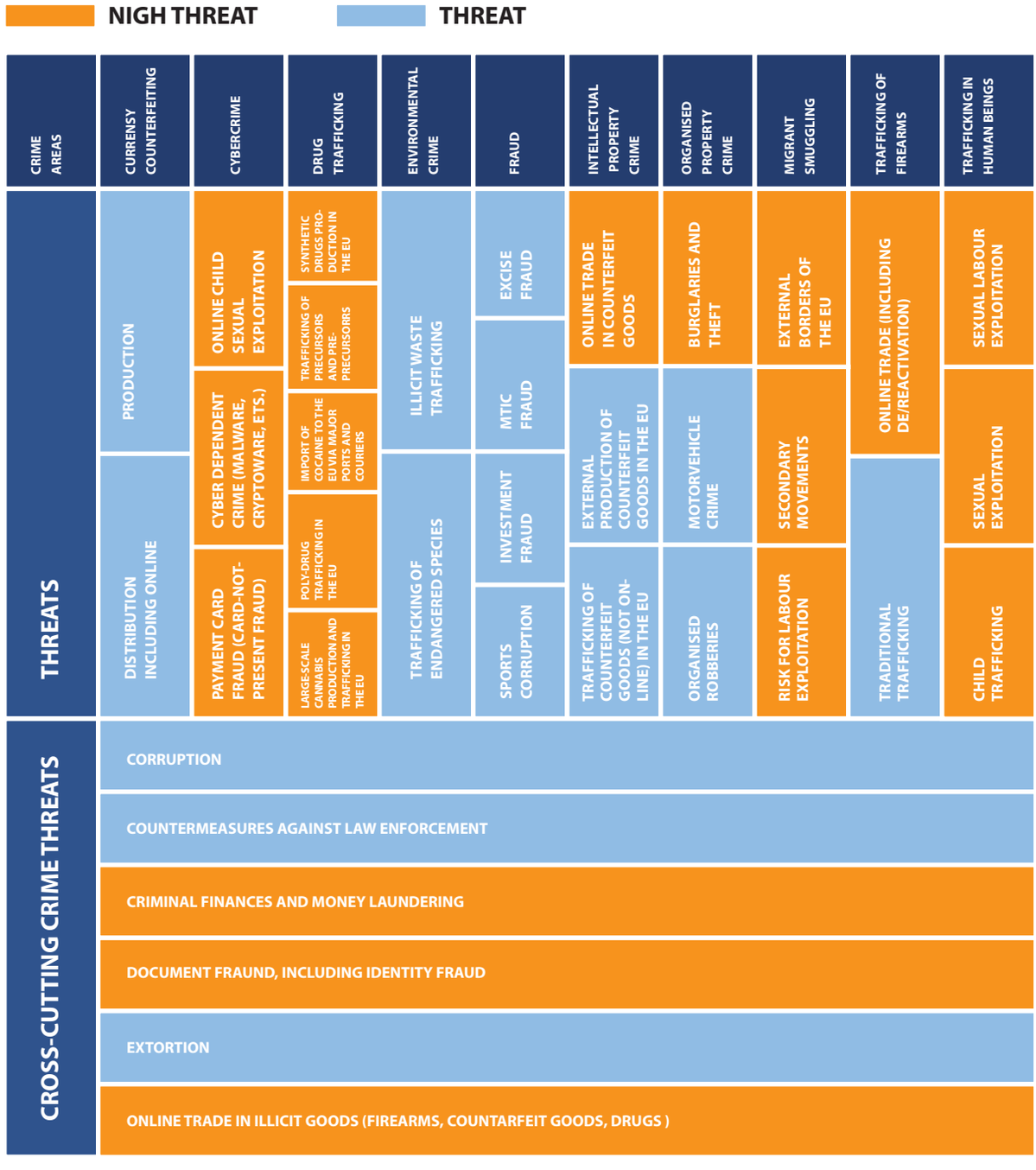
Впровадження норм Регламенту в українське законодавство має сприяти співпраці між правоохоронними органами України та країн ЄС, а також полегшити діяльність українського бізнесу, який працює з персональними даними європейців, наприклад, у сфері IT.

/

3. БОРОТЬБА З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

Співпраця з ЄС у сфері боротьби з організованою злочинністю є одним з положень статті 22 Угоди про асоціацію. Вона також передбачена Планом заходів з її реалізації.

Наразі Україна впроваджує європейську концепцію правоохоронної діяльності діяльності - Intelligence Led Policing (ILP). Її суть полягає у стратегічному та оперативному плануванні у сфері боротьби з оргзлочинністю. Зокрема, це передбачає кримінальний аналіз та оцінку ризиків. Аналітичний компонент в Україні ослаблений через обмежений доступ Нацполіції до спеціального програмного забезпечення та неналежну взаємодію правоохоронних структур щодо обміну інформацію, серед інших причин. Для його посилення Україна взяла на себе зобов'язання **запровадити методологію Європолу з оцінки загроз тяжких злочинів та організованої злочинності (SOCTA**) до 2023 року. Відповідні рекомендації надала також Консультативна місія ЄС в Україні. Ця методологія передбачає застосування якісних та кількісних методів дослідження для визначення найбільших кримінальних загроз. Ось, наприклад, таблиця із найбільш детального дослідження загроз організованої злочинності та тяжких злочинів у ЄС за 2017 рік:



Джерело: https://www.europol.europa.eu/socta/2017/conclusions.html

Водночас, Україна ще в процесі **написання Стратегії боротьби з організованою злочинністю.** Відповідно до планів уряду така стратегія та план дії на її виконання мають бути розробленими до кінця 2020 року і виконані до 2024 року.

Важливим елементом євроінтеграції України є налагодження співпраці з Європолом та іншими міжнародними інституціями у цій сфері. Для цього, зокрема, завершено процедуру ратифікації Меморандуму між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку.

На відміну від Інтерполу, до бази даних якого вже підключено 157 пунктів пропуску і який займається переважно створенням глобальних баз даних та проведенням спільних поліцейських операцій, Європол надає аналітичну, технічну та фінансову підтримку партнерам для попередження та боротьби з тяжкими злочинами та тероризмом.

Наявність сучасного обладнання є ще одним викликом для України. Воно потрібне для посилення спроможності українських правоохоронців у боротьбі з оргзлочинністю. Відповідну підтримку надає, наприклад, Євросоюзу у рамках проекту «Підтримка реформ у галузі верховенства права в Україні у сферах діяльності поліції, прокуратури та належного врядування» (ПРАВО-ІІ). Наприклад, у 2018 році Департамент стратегічних розслідувань Національної поліції України отримав 150 комп'ютерів та 20 принтерів.

В Україні постійно з'являються нові легальні наркотики. Вони легальні, бо не занесені до переліку наркотичних засобів, психотропних речовин і прекурсорів. Впроваджуючи європейські правила, 2019 року уряд прийняв постанову з питань проведення моніторингу наркотичної та алкогольної ситуації в Україні. Моніторинг проводить Центр психічного здоров'я і моніторингу наркотиків та алкоголю МОЗ за показниками, визначеними Європейським моніторинговим центром з наркотиків та наркотичної залежності (ЄМЦННЗ), Комісією з наркотичних засобів при ООН, Міжнародним комітетом з контролю за наркотиками. Він передбачає й співпрацю з правоохоронними органами для виявлення незаконного обігу психоактивних речовин та пов'язану з ним злочинність. Водночас, фахівці ЄМЦННЗ у рамках проекту ЄС EU4Monitoring Drugs поділились досвідом моніторингу через інтернет та дослідження стокових вод, які можуть містити залишки наркотичних речовин.

Проте досі **немає Порядку визнання засобів/речовин аналогами наркотичних засобів і психотропних речовин для забезпечення належної протидії появи у незаконному обігу нових психоактивних речовин,** створеного за результатами вивчення європейського досвіду з питань протидії незаконному обігу нових психоактивних речовин. Він має забезпечити швидку та ефективну процедуру занесення нових наркотиків до підконтрольного переліку наркотичних засобів, психотропних речовин і прекурсорів. Міністерство охорони здоров'я написало відповідний проект наказу.

Водночас, Україна прагне **приєднатися до системи раннього оповіщення Європейського Союзу щодо нових психоактивних речовин.** Таким чином, вона отримає доступ до інформації про нові наркотики, точки, де їх виробляють або торгують ними[1].

Також Україна взяла на себе зобов'язання **приєднатись до Групи зі співробітництва в боротьбі проти зловживання наркотиками та їх незаконним обігом (Група Помпіду), що має на меті зупинення незаконного вживання наркотиків і їх незаконного обігу.**

Виконання плану заходів на 2019-2020 роки з реалізації Стратегії державної політики щодо наркотиків на період до 2020 року, а також створення нового плану та стратегії до 2025 року сприятимуть подальшій євроінтеграції у цій сфері.

1 Приклади перший звітів в межах системи раннього оповіщення можна знайти за цим посиланням: http://www.emcdda.europa.eu/publications/topic-overviews/eu-early-warning-system

Для попередження торгівлі людьми та боротьби з нею Нацполіція висвітлює в українських медіа та соцмережах відеоролики про затримання злочинців. Відповідні сюжети виходять також на телеканалі "Еспресо" у програмі "Поліцейська хвиля". За 6 місяців 2019 року поліцейські викрили чотири організовані групи, які діяли у сфері торгівлі людьми. Україна також продовжує реалізацію Державної соціальної програми протидії торгівлі людьми на 2016—2020 роки.

У доповіді 2018 року Група експертів Ради Європи із протидії торгівлі людьми (GRETA) відзначила прогрес України у реалізації Конвенції Ради Європи про заходи щодо протидії торгівлі людьми. Водночас, у квадратних дужках пункту 240 ця Група відзначила **питання, які потребують негайного втручання.** Серед них, наприклад, активізація зусиль щодо запобігання торгівлі людьми з метою трудової експлуатації, а також торгівлі дітьми.

У сфері неврегульованої міграції Україна успішно виконує свої домовленості з ЄС щодо реадмісії. Вона **веде перемовини про укладення імплементаційних протоколів до Угоди між Україною та ЄС про реадмісію осіб, а також угоди про реадмісію осіб з державами походження (транзиту) неврегульованих мігрантів.**

Для боротьби з відмиванням коштів та фінансування тероризму Україна ухвалила новий закон "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення". Він адаптує українське законодавство до європейського: Директиви (ЄС) 2015/849 "Про запобігання використанню фінансової системи для відмивання грошей та фінансування тероризму" та Регламенту(ЄС) 2015/847 "Про інформацію, що супроводжує грошові перекази". Зокрема, спрощено процедури звітування про фінансові операції для суб'єктів первинного фінансового моніторингу (банків, страховиків, кредитних спілок, ломбардів, бірж, платіжних організацій та інших фінансових установ). Наприклад, поріг обов'язкового повідомлення про фінансові операції збільшено із 150 до 400 тис. грн., а кількість ознак таких операцій зменшено з 17 до 4. Водночас, закон передбачає ризик-орієнтований підхід при проведенні належної перевірки клієнтів та кейсове звітування про підозрілі операції. Він посилює вимоги до розкриття кінцевих бенефіціарних власників компаній, а також санкції.

Окрім того, продовжується **реалізація Стратегії розвитку системи запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення на період до 2020 року.**

Водночас, Україна взяла зобов'язання до 2024 року **укласти міжнародні договори (меморандуми) про співробітництво з питань протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму.**

Для розширення можливостей у протидії незаконному переміщенню через кордон активів здобутих злочинним шляхом та наркотиків Україна планує зобов'язати авіаперевізників передавати дані PNR (Passenger Name Record). Це дані картки, які пасажири вносять під час бронювання та купівлі квитка, і після чого отримують PNR номер. У Євросоюзу відповідне законодавство вже діє завдяки Директиві ЄС 2016/681 про використання системи обліку персональних даних пасажирів для запобігання, виявлення, розслідування тяжких злочинів та злочинів пов'язаних з тероризмом (passenger name record - PNR), яка набула чинності наприкінці травня 2018 року. **Транспозиція норм цієї Директиви в українське законодавство дозволить українським правоохоронним органам обмінюватися даними з країнами ЄС.**

Водночас, у 2018 році Консультативна місія ЄС **презентувала в Україні систему «Cash Team».** Вона передбачає створення в аеропортах та портах аналітичних відділів, які мають доступ до даних та аналітики від різних відомств (Національної поліції, Державної прикордонної служби, Служби безпеки України, Державної митної служби України), наприклад, записи системи обліку персональних даних пасажирів або свідчення про незаконний трафік готівки.

/

4. ПРОПОЗИЦІЇ

КІБЕРБЕЗПЕКА

- прийняти План заходів на 2020 рік із реалізації Стратегії кібербезпеки;
- ухвали закони та підзаконні акти на виконання Закону України "Про основні засади забезпечення кібербезпеки України".
- впровадити в українське законодавство норми Директиви ЄС щодо мережевої та інформаційної безпеки (директива NIS - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union). Серед іншого:
  - визначити, які саме об'єкти вважати критичною інфраструктурою та процедуру їх аудиту, або на рівні закону, або на рівні підзаконних актів;
  - визначити зобов'язання провайдерів цифрових послуг у сфері кібербезпеки;
  - прописати чіткий механізм державно-приватної взаємодії;
- укласти меморандуми про співпрацю з Європейським агентством з питань мережевої та інформаційної безпеки "ENISA", Трастовим фондом НАТО з кібербезпеки, Південно-Східним Європейським правоохоронним центром (SELEC);
- варто внести до Кримінально-процесуального кодексу визначення поняття електронних доказів та процедуру їх збору;
- впровадити в українське законодавство норми The EU Cybersecurity Act, зокрема нову схему сертифікації продуктів, процесів та послуг ICT;
- забезпечити конкурентну оплату праці для залучення фахівців із кібербезпеки.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

- **удосконалити законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679. Зокрема:**
- створити спеціальний незалежний наглядовий орган із захисту персональних даних;
- зобов'язати компанії отримувати чітку згоду користувачів на обробку даних;
- зобов'язати компанії призначити особу відповідальну за захист персональних даних (data protection officer - DPO), а також забезпечувати безпеку персональних даних (шифрування, псевдонімізація тощо);
- надати користувачу право "стирання" даних, якщо у них немає необхідності, користувач відкликає згоду на їх обробку, відсутній легітимний інтерес, або їх обробку здійснено незаконно;
- надати регулятору повноваження штрафувати компанії за порушення.

БОРОТЬБА З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

- запровадити методологію Європолу з оцінки загроз тяжких злочинів та організованої злочинності (SOCTA);
- розробити Стратегію боротьби з організованою злочинністю та план дії на її виконання;
- забезпечити правоохоронні органи потрібним обладнання для посилення спроможності у протидії оргзлочинності.

БОРОТЬБА З НАРКОЗЛОЧИННІСТЮ

- ухвалити Порядок визнання засобів/речовин аналогами наркотичних засобів і психотропних речовин для забезпечення належної протидії появи у незаконному обігу нових психоактивних речовин;
- приєднатися до системи раннього оповіщення Європейського Союзу щодо нових психоактивних речовин;
- приєднатись до Групи зі співробітництва в боротьбі проти зловживання наркотиками та їх незаконним обігом (Група Помпіду), що має на меті зупинення незаконного вживання наркотиків і їх незаконного обігу;
- продовжити виконання плану заходів на 2019-2020 роки з реалізації Стратегії державної політики щодо наркотиків на період до 2020 року; а також розробити новий план та стратегію до 2025 року.

ПРОТИДІЯ ТОРГІВЛІ ЛЮДЬМИ

- виконати рекомендації Групи експертів Ради Європи із протидії торгівлі людьми (GRETA), надані у пункті 240 доповіді 2018 року як питання, які потребують негайного втручання.

БОРОТЬБА З НЕВРЕГУЛЬОВАНОЮ МІГРАЦІЄЮ

- продовжувати перемовини про укладення імплементаційних протоколів до Угоди між Україною та ЄС про реадмісію осіб, а також угоди про реадмісію осіб з державами походження (транзиту) неврегульованих мігрантів.

ПРОТИДІЯ ВІДМИВАННЯ КОШТІВ ТА ФІНАНСУВАННЯ ТЕРОРИЗМУ

- продовжити реалізацію Стратегії розвитку системи запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення на період до 2020 року;
- укласти міжнародні договори (меморандуми) про співробітництво з питань протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму.
- впровадити в законодавство норми Директиви ЄС 2016/681 про використання системи обліку персональних даних пасажирів для запобігання, виявлення, розслідування тяжких злочинів та злочинів пов'язаних з тероризмом;
- створити в аеропортах та портах cash teams у співпраці з КМЄС.