ЗАТВЕРДЖУЮ
Голова ГО «Проти Корупції»
_____ Путря Ю.М.
«23» березня 2024

ПОЛІТИКА ЗАПОБІГАННЯ ФІНАНСУВАННЮ ТЕРОРИЗМУ

(Counter-Terrorism Financing Policy)

Громадської організації «Проти Корупції»

м. Корсунь-Шевченківський

І. Загальні положення

1.1. Політика запобігання фінансуванню тероризму (далі — Політика) Громадської організації «Проти Корупції» (далі — Організація) визначає загальні вимоги, стандарти та процедури, спрямовані на **недопущення** будь-якого прямого чи опосередкованого залучення Організації до фінансування тероризму, фінансування розповсюдження зброї масового знищення та інших форм фінансування протиправної діяльності.

1.2. Ця Політика поширюється на **всі фінансові та ділові відносини Організації** — з донорами, партнерами, ґрантерами, субґрантерами, підрядниками, постачальниками, консультантами, працівниками, волонтерами, бенефіціарами, а також на всі внутрішні операції.

1.3. Цілі Політики:

- забезпечення відсутності будь-яких зв'язків Організації з фінансуванням тероризму та розповсюдження зброї масового знищення;
- дотримання санкційних режимів України, ООН, США, ЄС, Великої Британії, Канади, Австралії, Японії та інших юрисдикцій, стандарти яких є обов'язковими для Організації або її донорів;
- виконання вимог законодавства України, зокрема **Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»** № 361-IX від 06.12.2019;
- відповідність міжнародним стандартам **Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF)**, зокрема Рекомендації 8 щодо неприбуткових організацій;
- виконання вимог донорів (NORAD, SIDA, ЄС, USAID та інших) щодо антитерористичного контролю;
- захист Організації від репутаційних, юридичних та фінансових ризиків, пов'язаних з несвідомим використанням її ресурсів у протиправних цілях.

1.4. Ця Політика діє одночасно з:

- Політикою комплексної перевірки партнерів та ґрантерів (Due Diligence);
- Антикорупційною політикою;
- Політикою протидії шахрайству та хабарництву;
- Положенням про фінансове управління;
- Положенням про закупівлі;
- Політикою безпеки.

1.5. **Нульова толерантність.** Організація декларує принцип **абсолютної нетерпимості** до будь-яких форм фінансування тероризму, підтримки терористичних чи екстремістських угруповань, а також до фінансування розповсюдження зброї масового знищення. Жодні виправдання (гуманітарні, безпекові, оперативні) не можуть бути підставою для порушення цієї Політики.

1.6. Оскільки Україна перебуває у стані повномасштабної війни з Російською Федерацією, яка активно фінансує терористичну діяльність в Україні та в інших країнах, дотримання цієї Політики є питанням не лише правового та етичного характеру, а й **питанням національної безпеки**.

II. Терміни та визначення

Фінансування тероризму — надання чи збирання будь-яких активів (грошових коштів, майна, послуг) з усвідомленням того, що вони будуть використані повністю чи частково для вчинення будь-якого терористичного акту, а також для фінансування або матеріального забезпечення особи, яка вчиняє терористичний акт, або терористичної групи (терористичної організації).

Фінансування розповсюдження зброї масового знищення — надання, збирання, використання активів для розроблення, придбання, виробництва, володіння, перевезення, розповсюдження або застосування ядерної, хімічної, біологічної, радіологічної зброї, засобів її доставки, а також пов'язаних матеріалів та технологій.

Терористичний акт — застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини, заподіяння шкоди майну, з метою залякування населення, провокації воєнного конфлікту, впливу на прийняття рішень органами державної влади (див. Кримінальний кодекс України).

Терористична організація (група) — стійке об'єднання осіб для здійснення терористичної діяльності.

Санкційні списки — переліки осіб, юридичних осіб, організацій, до яких застосовані обмежувальні заходи (санкції) міжнародними організаціями, окремими державами або Україною.

Заморожування активів — заборона на здійснення операцій або зміну складу активів визначених осіб та організацій.

Клієнтська належна перевірка (Customer Due Diligence, CDD) — процес ідентифікації та верифікації особи ділового партнера, оцінки ризиків співпраці з ним.

Підозріла операція — операція, характер, обсяг, час або учасники якої дають підстави вважати, що вона може бути пов'язана з фінансуванням тероризму, розповсюдженням ЗМЗ або відмиванням коштів.

Уповноважений орган України — Державна служба фінансового моніторингу України (Держфінмоніторинг), а також Служба безпеки України у частині запобігання терористичній діяльності.

Відповідальний працівник — особа Організації, призначена для реалізації цієї Політики (менеджерка проєктів — Карина Арбузова).

III. Категорії ризику

3.1. В Організації встановлюються **три категорії ризику**, згідно з якими визначається рівень перевірки ділових партнерів та інтенсивність моніторингу:

1) Високий ризик: ділові партнери, що потрапляють до цієї категорії, підлягають найвищому рівню перевірок та **регулярному щомісячному моніторингу**.

2) Середній ризик: ділові партнери, що вважаються менш ризиковими за високоризикових, підлягають поглибленим перевіркам та **регулярному щоквартальному моніторингу**.

3) Низький ризик: ділові партнери з мінімальним рівнем ризику підлягають стандартним перевіркам та **щорічному моніторингу**.

3.2. Для віднесення ділового партнера до категорії ризику застосовуються такі критерії:

Географічне розташування — партнери, які зареєстровані, ведуть діяльність або мають бенефіціарних власників у країнах (юрисдикціях) з високим рівнем ризику:

- країни-агресори (Російська Федерація, Республіка Білорусь);
- країни зі спеціальними санкційними режимами ООН/ЄС/США (Іран, КНДР, Сирія, М'янма тощо);
- країни, включені до **сірого/чорного списку FATF** (актуальний перелік — на fatf-gafi.org);
- юрисдикції з високим рівнем корупції за індексом Transparency International;
- офшорні юрисдикції.

Вид діяльності — партнери, що здійснюють господарську діяльність з підвищеним ризиком:

- оборонна промисловість, торгівля зброєю чи товарами подвійного використання;
- фінансові послуги, крипто-активи, обмін валют;
- благодійні організації з невідомою або непрозорою структурою;
- юридичні особи з невідомими або складними ланцюжками власності;
- організації, що працюють у зонах активних бойових дій або на тимчасово окупованих територіях.

Фінансові показники — партнери, які здійснюють:

- значні за обсягами фінансові операції (понад 1 млн грн разово або 5 млн грн річно);
- готівкові операції на значні суми;
- операції з нестандартними структурами платежів (транзитні платежі, невідповідність між заявленою діяльністю та фінансовими потоками);
- швидкі перекази коштів через кілька юрисдикцій.

Тип особи:

- **Публічні діячі (PEP)** та їхні пов'язані особи (родичі, ділові партнери);
- особи, що фігурували у медіа-повідомленнях про зв'язки з терористичною або екстремістською діяльністю (навіть за відсутності судових рішень);
- фізичні особи або юридичні особи з громадянством/реєстрацією РФ або Білорусі (крім осіб, які отримали статус біженця в Україні або мають публічно підтверджену опозиційну позицію).

3.3. Партнер може бути автоматично віднесений до **високої категорії ризику**, якщо хоча б за одним критерієм має ознаку високого ризику.

3.4. Особливості умов та порядок визначення категорій ризику детально описано у Політиці Due Diligence (Розділ 7 та Додаток 3 — Матриця ризиків).

IV. Обов'язкові та додаткові перевірки

4.1. **Обов'язкова перевірка** застосовується до кожного ділового партнера, донора, ґрантера, працівника, волонтера та бенефіціара, який отримує суттєві матеріальні цінності, — **незалежно від категорії ризику**.

4.2. Обов'язкова перевірка проводиться на предмет наявності інформації про партнера щодо його причетності до **терористичної діяльності** або застосування щодо нього економічних санкцій України, інших держав чи організацій, рішення і акти яких є юридично обов'язковими. Зокрема, але не виключно, перевіряється наявність партнера у таких списках:

- **Санкційний список Ради Безпеки ООН** (Consolidated United Nations Security Council Sanctions List);
- **Санкційний список Європейського Союзу** (EU Consolidated Financial Sanctions List, EU Sanctions Map);
- **Санкційний список Великої Британії** (UK Sanctions List);
- **Санкційний список Міністерства фінансів США — OFAC** (Specially Designated Nationals and Blocked Persons List);
- **Санкційні списки Бюро промисловості та безпеки США (BIS)** — Entity List, Denied Persons List, Unverified List;
- **System for Award Management (SAM.gov)** — список осіб, яким заборонено отримувати фінансування або укладати угоди з американськими організаціями;
- **Санкційний список Канади** (Consolidated Canadian Autonomous Sanctions List);
- **Зведений санкційний список Австралії**;
- **Санкційний список Японії** проти Російської Федерації;
- **Санкційний портал СНБО України** (sanctions.nazk.gov.ua);

- **Реєстр терористів Держфінмоніторингу України** (перелік осіб, пов'язаних із здійсненням терористичної діяльності або щодо яких застосовано міжнародні санкції);
- **Списки FATF щодо високоризикових юрисдикцій та тих, що знаходяться під моніторингом**;
- **Реєстр НАЗК** осіб, які вчинили корупційні правопорушення (додатково).

4.3. **Ділові відносини не можуть бути встановлені** з партнером у разі, якщо:

- партнер причетний до терористичної діяльності;
- партнер включений до будь-якого з переліків, наведених у пункті 4.2;
- бенефіціарний власник, керівник або підписант партнера відповідає критеріям пункту 4.2;
- партнер зареєстрований на тимчасово окупованих територіях України.

Установлені ділові відносини у таких випадках **негайно припиняються**, а активи заморожуються у встановленому законом порядку.

4.4. **Додаткова перевірка** здійснюється щодо партнерів середнього та високого рівнів ризику на наявність:

- участі у попередніх кримінальних провадженнях, пов'язаних з фінансовими злочинами, тероризмом, екстремізмом;
- медіа-експозиції із зв'язками з підозрілими особами або організаціями;
- співпраці з юридичними особами з санкційних юрисдикцій;
- нетипових фінансових потоків.

V. Заходи перевірки

5.1. Заходи перевірки складаються з трьох компонентів:

- процедура ідентифікації партнера;
- автоматизована перевірка;
- ручна перевірка.

5.2. **Процедура ідентифікації партнера** полягає в отриманні основної інформації про ділового партнера, а саме:

- офіційне найменування;
- реєстраційні дані (ЄДРПОУ / ІПН / реєстраційний номер у своїй країні);
- перелік засновників (учасників);
- кінцевий бенефіціарний власник (з часткою від 25%);
- відомості про структуру власності (у тому числі непряме володіння);
- види діяльності (за КВЕД, номенклатурою або іншим класифікатором);
- місцезнаходження (юридична та фактична адреси).

Ця процедура включає використання відкритих джерел та баз даних для отримання додаткової інформації, зокрема перевірку історії організації, публікацій в медіа та репутації у діловому та громадському середовищі.

5.3. **Автоматизована перевірка** полягає у використанні спеціалізованих програмних засобів для перевірки партнера в автоматизованих інформаційних та довідкових системах, реєстрах, базах даних:

- YouControl / OpenDataBot (Україна);
- інтегровані сервіси перевірки санкційних списків (за наявності доступу);
- вбудовані інструменти системи Odoo для перевірки контрагентів;
- Єдиний державний реєстр юридичних осіб (за API або через веб-сервіс).

Спеціалізовані програмні засоби мають забезпечувати **оперативне сповіщення** відповідального працівника Організації у разі виявлення підозрілої діяльності або потрапляння партнера у переліки осіб, до яких застосовано санкції або які пов'язані з провадженням терористичної діяльності.

5.4. **Ручна перевірка** застосовується відповідальним працівником (менеджеркою проєктів) як додаткова у разі, якщо автоматизована перевірка не надає достатньої інформації або виникають сумніви щодо наданих результатів.

За потреби можуть проводитися:

- додаткові інтерв'ю з представниками партнера;
- опитування щодо ділової практики, репутації, відповідності діяльності законодавству України;
- запити до попередніх партнерів або донорів;
- юридичні консультації;
- співпраця з фахівцями Держфінмоніторингу або СБУ (у виняткових випадках, за погодженням Голови організації).

5.5. Порядок проведення перевірок при здійсненні процедур закупівель, укладенні ґрант-угод з субґрантерами та інших форм співпраці, а також шаблони оформлення результатів перевірок визначаються **Політикою Due Diligence** ГО «Проти Корупції» та її Додатками (Чек-лист DD, Форма самодекларації, Матриця ризиків).

VI. Моніторинг

6.1. Організацією здійснюється **регулярний моніторинг** ділових партнерів та моніторинг змін щодо них.

6.2. Періодичність регулярного моніторингу залежно від категорії ризику:

1) Партнери з високим рівнем ризику — щомісяця. Об'єкти моніторингу:

- зміни у структурі власності;

- зміни у складі керівних органів;
- зміни у фінансових показниках;
- зміни у діловій практиці;
- поява у санкційних списках або медіа-повідомленнях;
- зміни у статусі юридичних облікових даних.

2) Партнери з середнім рівнем ризику — щоквартально. Основний акцент — фінансові показники, структура власності, регуляторні вимоги.

3) Партнери з низьким рівнем ризику — раз на рік. Перевірка на відповідність вимогам законодавства України та внутрішнім політикам Організації.

6.3. **Моніторинг змін** здійснюється:

1) Для перевірки змін у структурі власності партнера. Особлива увага приділяється у разі появи нових бенефіціарних власників або змін у складі керівних органів (наприклад, поява громадян країн-агресорів у складі керівництва).

2) Для оновлення баз даних про партнерів з метою підтримання в актуальному стані достовірної інформації про них — у системі Odoo та у справі партнера.

6.4. **Санкційний скринінг** проводиться:

- **до укладення** будь-якого договору (обов'язковий первинний);
- **при зміні** ключових параметрів партнерства (нові підписанти, зміна структури, укладення додаткових угод);
- **щорічно** для всіх довгострокових партнерів (плановий);
- **позапланово** — за появи інформації про можливе включення до санкційних списків або зв'язки з терористичною діяльністю.

6.5. Результати кожного моніторингу оформлюються у Звіті моніторингу партнера, що зберігається у справі партнера у системі Odoo.

VII. Виявлення підозрілих операцій та реагування

7.1. Кожен працівник, підрядник, волонтер Організації **зобов'язаний повідомляти** про будь-які операції або обставини, що можуть свідчити про фінансування тероризму або пов'язану з ним діяльність. Зокрема, тривожними є такі ознаки:

- прохання партнера здійснити платіж в іншу країну, ніж країна реєстрації партнера;
- прохання про поділ платежу на кілька дрібних траншів без економічного обґрунтування;
- надходження коштів з невідомих або підозрілих джерел;
- пропозиції готівкових розрахунків на значні суми;

- надходження коштів через юрисдикції з підвищеним ризиком (сірий/чорний список FATF);
- невідповідність між заявленою діяльністю партнера та фактичними фінансовими потоками;
- відмова партнера надати основну ідентифікаційну інформацію або документи;
- складна структура власності без прозорого пояснення;
- партнер наполягає на анонімності або конфіденційності операцій;
- підозри у зв'язках керівництва партнера з проросійськими організаціями або особами;
- виявлення в медіа інформації про можливі зв'язки партнера з терористичною діяльністю.

7.2. **Порядок повідомлення:**

Крок 1. Працівник **негайно** припиняє відповідну операцію або утримується від прийняття рішення щодо її здійснення.

Крок 2. Працівник у той же робочий день письмово (або через захищений канал — Signal) повідомляє **менеджерку проєктів** (Уповноважену особу) та **Голову організації**.

Крок 3. Менеджерка проєктів проводить оперативний аналіз ситуації протягом 24 годин та готує **Оперативний звіт** із детальним описом.

Крок 4. Голова організації ухвалює рішення про:

- припинення операції та інформування партнера;
- заморожування активів на рахунках;
- повідомлення уповноважених органів (Держфінмоніторингу України, СБУ, Національної поліції України — залежно від характеру ситуації);
- інформування донора, якщо ситуація стосується його коштів;
- юридичне супроводження ситуації.

7.3. **Заборонено**:

- продовжувати операцію без ухваленого рішення Голови організації;
- інформувати партнера (об'єкт підозри) про факт розслідування (принцип «tipping off» — заборона попередження підозрюваних);
- знищувати або приховувати документацію, пов'язану з підозрілою операцією.

7.4. **Захист працівника, який повідомив.** Працівник, який добросовісно повідомив про підозрілу операцію, отримує повний захист від будь-яких негативних наслідків (звільнення, тиск, зміна умов роботи) — відповідно до Антикорупційної політики (Розділ VIII щодо захисту викривачів).

VIII. Ідентифікація донорів

8.1. **Особлива увага приділяється перевірці донорів** — джерел фінансування діяльності Організації. Це є критично важливим, оскільки прийняття коштів з підозрілого або незаконного джерела може автоматично зробити Організацію учасником схеми фінансування тероризму або відмивання коштів.

8.2. **Обов'язково перевіряються:**

- усі нові донори перед укладенням першої ґрант-угоди (Поглиблений рівень DD, згідно з Політикою Due Diligence);
- нові приватні донори (фізичні та юридичні особи), які здійснюють пожертви понад 50 000 грн;
- усі анонімні пожертви понад 5 000 грн (в такому випадку — від таких пожертв краще утриматися або повернути кошти);
- будь-які надходження з нестандартних джерел (криптовалюти, готівка, іноземні перекази з юрисдикцій підвищеного ризику).

8.3. **Заборонено приймати кошти від:**

- фізичних та юридичних осіб, зареєстрованих у РФ, Білорусі, Ірані, КНДР та інших санкційних юрисдикціях;
- осіб, включених до санкційних списків України, ООН, США, ЄС, Великої Британії;
- осіб, зареєстрованих на тимчасово окупованих територіях України;
- осіб, які фігурують у розслідуваннях щодо фінансування тероризму;
- осіб, походження коштів яких неможливо задокументувати або пояснити.

8.4. У разі виявлення такого джерела на етапі, коли кошти вже надійшли, — Організація **негайно повертає** ці кошти (у разі можливості) або передає до Держбюджету у порядку, встановленому законодавством, з обов'язковим повідомленням Держфінмоніторингу.

IX. Відповідальність та звітність

9.1. **Голова організації:**

- забезпечує загальну реалізацію цієї Політики;
- затверджує рішення про припинення операцій, заморожування активів, повідомлення уповноважених органів;
- підписує звіти до Держфінмоніторингу та інших органів;
- є персонально відповідальним перед донорами та державними органами за дотримання антитерористичних вимог.

9.2. **Менеджер/ка проєктів** — призначається **Відповідальним працівником** з питань запобігання фінансуванню тероризму:

- координує реалізацію цієї Політики на щоденній основі;
- проводить санкційний скринінг усіх нових партнерів та донорів;
- веде реєстр перевірених партнерів у системі Odoo;
- готує щоквартальні та річні звіти Голові організації;
- організовує навчання команди;
- є першою точкою контакту у випадках підозрілих операцій;
- підтримує зв'язок з Держфінмоніторингом (за потреби).

9.3. **Фінансовий менеджер:**

- відповідальна за фінансовий контроль всіх операцій через систему Odoo;
- забезпечує подвійний контроль транзакцій понад 50 000 грн;
- інформує Уповноважену особу про будь-які нестандартні фінансові операції;
- готує фінансові звіти для Держфінмоніторингу у разі потреби.

9.4. **Керівники напрямів та проєктів:**

- ініціюють перевірки партнерів згідно з Політикою Due Diligence;
- інформують Уповноважену особу про будь-які підозри;
- дотримуються обмежень та правил цієї Політики у своїх напрямах.

9.5. **Усі працівники, підрядники, волонтери:**

- зобов'язані дотримуватися вимог цієї Політики;
- зобов'язані повідомляти про будь-які підозрілі операції;
- зобов'язані проходити щорічне навчання.

Особи, винні у недотриманні вимог цієї Політики, несуть **дисциплінарну, адміністративну та кримінальну відповідальність** відповідно до законодавства України.

9.6. **Регулярна звітність:**

- **Щоквартальний звіт** Уповноваженої особи Голові організації — про проведені перевірки, виявлені ризики, вжиті заходи;
- **Річний звіт** Голови організації Загальним зборам — про стан виконання Політики, статистику перевірок, ризики;
- **Оперативний звіт** — негайно у разі виявлення порушень або значних ризиків, з детальним описом ситуації та рекомендаціями.

9.7. **Обов'язкове повідомлення уповноважених органів:**

- Держфінмоніторинг України — у разі виявлення підозрілих операцій, що містять ознаки фінансування тероризму або відмивання коштів;
- СБУ — у разі виявлення інформації, що може свідчити про терористичну діяльність;

- Національна поліція України — у разі виявлення інших кримінальних правопорушень.

Повідомлення здійснюється у порядку та у строки, встановлені Законом України №361-IX від 06.12.2019.

X. Навчання

10.1. Усі працівники, підрядники (за необхідністю) та волонтери, залучені до перевірки ділових партнерів або управління фінансовими ресурсами Організації, проходять **навчання з питань запобігання фінансуванню тероризму не рідше одного разу на рік**.

10.2. Навчання може включати різні формати:

- роз'яснення процедур цієї Політики та Політики Due Diligence;
- ознайомлення з оновленнями нормативних актів (Закон №361-IX, підзаконні акти, зміни санкційних режимів);
- практичні кейси (у тому числі анонімізовані реальні кейси зі сфери НГО);
- тренінги (внутрішні та зовнішні);
- онлайн-курси (у тому числі курси Держфінмоніторингу, IsUcode, спеціалізовані ресурси);
- ознайомлення з рекомендаціями FATF щодо неприбуткових організацій.

10.3. Проходження навчання фіксується у журналі обліку та у файлі працівника у системі Odoo.

10.4. Нові працівники проходять **вступний інструктаж** з питань цієї Політики протягом першого тижня роботи, до допуску до фінансових операцій.

XI. Заключні положення

11.1. Ця Політика підтримується в актуальному стані та переглядається **не рідше одного разу на рік** з метою вдосконалення системи перевірки та моніторингу ділових партнерів, а також у разі змін у законодавстві України, оновлення санкційних режимів або рекомендацій FATF.

11.2. Про результати щорічного перегляду Уповноважена особа (менеджерка проєктів) інформує Голову організації, а той — Загальні збори.

11.3. За потреби зміни до цієї Політики оформлюються шляхом внесення окремих змін або шляхом викладення Політики у новій редакції.

11.4. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, зокрема у зв'язку з прийняттям нових нормативно-правових актів, **Політика діє лише в тій частині, яка не суперечить чинному законодавству**.

11.5. Ця Політика оприлюднюється на офіційному сайті Організації **protucor.com** з метою підтвердження публічної відданості Організації принципам протидії фінансуванню тероризму.

11.6. Матеріали, зібрані у процесі реалізації цієї Політики (звіти, чек-листи, самодекларації, скриншоти реєстрів), зберігаються у зашифрованому вигляді у системі Odoo мінімум **5 років** після завершення співпраці з партнером (у відповідності до вимог Закону №361-IX).

Додатки

- **Додаток А.** Перелік санкційних списків з посиланнями на офіційні джерела (актуалізується щорічно).
- **Додаток Б.** Форма Оперативного звіту про підозрілу операцію.
- **Додаток В.** Форма Заяви про наявність/відсутність зв'язків з санкційними особами (для нових працівників та підрядників).
- **Додаток Г.** Чек-лист санкційного скринінгу (координується з Політикою Due Diligence).