МЕМОРАНДУМ ПРО ВЗАЄМОРОЗУМІННЯ
між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку

Україна

для цілей цього Меморандуму про взаєморозуміння представлена в особі Міністра внутрішніх справ (далі – «Міністерство»)

та

Європейський поліцейський офіс

для цілей цього Меморандуму про взаєморозуміння представлений в особі Директора (далі – «Європол»),

далі разом як «Сторони» або окремо як «Сторона»,

керуючись Угодою між Україною та Європейським поліцейським офісом про стратегічне співробітництво від 4 грудня 2009 року (далі – «Угода про співробітництво»),

зважаючи на те, що обмін інформацією між Сторонами на підставі Угоди про співробітництво передбачає встановлення захищеної лінії зв'язку між ними,

враховуючи намір Сторін посилити співробітництво шляхом укладання угоди про оперативне співробітництво в майбутньому,

домовились про таке:

Стаття 1

Мета

Метою цього Меморандуму про взаєморозуміння є врегулювання порядку встановлення, введення в дію та експлуатації захищеної лінії зв'язку для обміну інформацією між Сторонами.

Стаття 2

Обмін інформацією

1. Обмін інформацією між Сторонами повинен здійснюватися тільки згідно з законодавством України, відповідними правовими актами Європолу та відповідними положеннями Угоди про співробітництво.
2. Передача інформації з обмеженим доступом захищеною лінією зв'язку обмежена ступенем доступу до інформації RESTREINT UE/EU RESTRICTED (ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ) та її еквівалентом в Україні.

Стаття 3

Кодекс Зв'язку

1. Обидві Сторони зобов'язуються дотримуватись мінімальних стандартів безпеки, закріплених у Додатку 1 до цього Меморандуму про взаєморозуміння («Кодекс Зв'язку для захищеної мережі Європолу», далі – «Кодекс зв'язку»). Обидві Сторони підтверджують, що вони захистили системи зв'язку відповідно до базових стандартів безпеки оптимальними стратегіями та технологіями, а також врахували міри захисту, закріплені в Кодексі зв'язку.
2. Шляхом підписання цього Меморандуму про взаєморозуміння, Міністерство погоджується із Заявою про дотримання Кодексу Зв'язку, яка регулюється пунктом 1.4. частини D Кодексу зв'язку.
3. У випадку, якщо одна зі Сторін істотно ухиляється від виконання принципів та положень, визначених даною статтею або Кодексом зв'язку, зв'язок між двома мережами може бути припинено, доки дані питання не будуть вирішені.
4. Обидві Сторони погоджуються, що подальше з'єднання з будь-якою іншою мережею має бути закріплено в схожій угоді (Кодекс зв'язку), яка обумовить базовий захист такого з'єднання.
5. Обидві Сторони погоджуються не втручатись в інформаційно-комунікаційні системи одна одної, не здійснювати підключення чи відключення кабелів, обладнання до отримання чітких вказівок або до настання надзвичайної ситуації.
6. У випадку виникнення серйозної проблеми в системі безпеки, такої як, наприклад, зараження вірусом, Сторона повинна від'єднатись від системи іншої Сторони з метою запобігання подальшого поширення будь-якого вірусу.
7. Перед внесенням будь-яких змін в мережеві системи, які пов'язані з мережею іншої Сторони або які впливають на поточне з'єднання, необхідно надати попереднє письмове повідомлення керівнику Ресурсного Департаменту Європолу у випадку, коли це стосується Європолу, та відповідному Контактному пункту, призначеному для реалізації положень цього Меморандуму про взаєморозуміння, якщо це стосується Міністерства. Якщо виникне необхідність в робочій зустрічі з даного питання, вона має бути проведена, перш ніж будуть здійснені будь-які зміни.
8. Обидві Сторони домовляються використовувати системи зв'язку лише задля мети, вказаної у цьому Меморандумі про взаєморозуміння.

9. Кожна Сторона відповідає за захист власних систем, починаючи з демаркаційної точки.

10. Обидві Сторони погоджуються не здійснювати жодних видів перевірок, сканувань на пошук прогалин або втручань в інші системи без попереднього дозволу іншої Сторони.

11. Обидві Сторони погоджуються ділитись інформацією щодо загроз та прогалин, які можуть впливати на інші системи.

12. Обладнання Європолу, встановлене в приміщеннях Міністерства, є власністю Європолу. Обладнання Міністерства, встановлене в приміщеннях Європолу, є власністю Міністерства. Власник обладнання відповідає за його захист, однак залежно від обставин можуть укладатися двосторонні угоди, що містять виключення з цього принципу.

13. Кожна Сторона відповідає за стан власного обладнання. З метою вирішення питань щодо технічної підтримки та обслуговування системні адміністратори мережі кожної зі Сторін можуть складати відповідні запити. Процедура розгляду таких запитів регулюватиметься на двосторонній основі між Міністерством та Європолом.

Стаття 4

Закупка, утримання та розподіл коштів

1. Відповідно до правил закупівлі товарів, Європол здійснює закупки всіх товарів та послуг, необхідних для встановлення, введення в дію та експлуатації захищеної лінії зв'язку.

2. Витрати на встановлення захищеної лінії зв'язку також оплачуються Європолом. Захищена лінія зв'язку та все обладнання, пов'язане з нею, надаються Європолом та залишаються у власності Європолу.

3. Європол відповідає за функціонування захищеної лінії зв'язку та, якщо це необхідно, за заміну пошкодженого обладнання. Міністерство, відповідно до існуючих правил, забезпечує доступ уповноваженого Європолом персоналу до необхідних приміщень з метою здійснення технічної підтримки та заміни пошкодженого обладнання. У випадку виявлення Міністерством несправностей, необхідно першочергово звертатись по технічну допомогу до персоналу підрозділу Європолу з підтримки користувачів.

4. Щомісячні експлуатаційні витрати на захищену лінію зв'язку розподіляються між Сторонами навпіл, тобто кожна Сторона сплачує 50% від вартості. Європол буде сплачувати наперед всі необхідні щомісячні експлуатаційні витрати. Міністерство відшкодовуватиме 50% від щомісячних фактично понесених експлуатаційних витрат згідно з виставленим Європолом рахунком на відшкодування витрат на щоквартальній основі згідно з Фінансовими Правилами Європолу.

5. Якщо захищена лінія зв'язку буде демонтована, Міністерство повертає в Європол майно, яке є власністю Європолу, а Європол повертає до Міністерства майно, яке є власністю Міністерства.

6. Усі предмети імпорту та, у разі потреби, експорту Європолу повинні мати можливість безперешкодно доставлятись до або вивозитись з України, не підпадаючи під митні, імпортні або експортні збори, повинності, ПДВ або податки аналогічного характеру. Таке виключення застосовується лише до ввозу або вивозу товарів, пов'язаних з обладнанням, що постачається або повертається, та/або сервісом, що надається Європолом відповідно до цього Меморандуму про взаєморозуміння.

Стаття 5

Відповідальність та врегулювання спірних питань

1. Не обмежуючи зміст Статті 13 Угоди про співробітництво, Сторона несе відповідальність за шкоду, спричинену іншій Стороні в результаті встановлення, введення в дію або експлуатації захищеної лінії зв'язку. В таких випадках Сторони намагаються знайти справедливе розв'язання питання щодо компенсації збитків постраждалій Стороні.

2. Будь-які спірні питання між Сторонами стосовно тлумачення або застосування положень цього Меморандуму про взаєморозуміння повинні вирішуватись відповідно до статті 14 Угоди про співробітництво.

Стаття 6

Поправки

Зміни до цього Меморандуму про взаєморозуміння повинні бути взаємопогоджені в письмовій формі між Сторонами.

Стаття 7

Припинення дії

Дію цього Меморандуму про взаєморозуміння може бути припинено шляхом надсилання письмового повідомлення будь-якою Стороною за три місяці до цього.

Стаття 8

Набрання чинності та підписи

Цей Меморандум про взаєморозуміння набирає чинності в день, коли Україна повідомить Європолу в письмовій формі дипломатичними каналами про закінчення внутрішньодержавних процедур, необхідних для набрання чинності Меморандуму про взаєморозуміння.

Цей Меморандум про взаєморозуміння складено і підписано у двох примірниках українською та англійською мовами, кожен текст є рівноавтентичним. У разі виникнення невідповідностей щодо тлумачення статей, переважну силу матиме примірник англійською мовою.

м. Київ

Дата підписання 11.03.2015

За Україну

Арсен Аваков

Міністр внутрішніх справ України

м. Гаага

Дата підписання 19/3/15

За Європол

Роб Уейнрайт

Директор

1. Додаток 1: Кодекс Зв'язку

1.1 Частина А: Вступ

Первинна мета даного Кодексу Зв'язку (CoCo) полягає в забезпеченні того, що Захищена мережа Європолу та зовнішні мережі (Партнерські Установи), які пов'язані між собою, достатньо захищені від загроз конфіденційності, цілісності та доступу до інформації. Відомо, що проблема в системах захисту в мережі однієї Партнерської Установи або Європолу потенційно може вплинути на взаємопов'язані мережі всіх інших Партнерських Установ.

Головний принцип цього Кодексу Зв'язку полягає в тому, що всі Партнерські Установи, підключені до Захищеної мережі Європолу, повинні дотримуватись мінімального набору заходів контролю безпеки. Такий принцип захисту спрямований на те, щоб зменшити до прийнятного рівня, визначеного відповідним підрозділом по забезпеченню безпеки, ризик в сфері захисту будь-якої з систем від впливу та залежності від безпеки цілої мережі. Кожна Партнерська Установа відповідає за безпеку власних систем, починаючи з демаркаційної точки.

Кодекс Зв'язку є обов'язковим для Європолу та Партнерської Установи. Поняття, принципи, контроль та зобов'язання, вказані в ньому, повинні виконуватись та поважатись.

1.2. Частина В: Базові стандарти контролю безпеки

1.2.1. Система особливих вимог Європолу до захисту мережевих систем

Європол визначає перелік вимог з безпеки мережевої інфраструктури в документі, що називається "Система особливих вимог Європолу до захисту мережевих систем" (SSSR) документ № 2440-72". Даний документ чітко та повністю закріплює принципи захисту, яких слід дотримуватись та детальні вимоги з безпеки системи. Він базується на основних принципах безпеки, описаних в Посібнику з безпеки Європолу, та на основі системи оцінювання ризиків.
Система Захисту Європолу SSSR була прийнята Адміністративною Радою за рекомендацією Комітету з Безпеки Європолу. Цей документ підлягає регулярним переглядам та оновленню в контексті переакредитації системи.
Обов'язковою вимогою до зв'язку між зовнішніми мережами та Системою Захисту Європолу є те, що Україна та Європол зобов'язані запроваджувати політику, процедури та технічні заходи подібні до тих, що зазначаються в документі SSSR. Це не означає, що існуючі процедури та технології мають бути ідентичними, але ідеї, які згадуються в даному документі, повинні відповідати національній політиці та правилам. Це також підпадає під дію статті 2 «Правил конфіденційності інформації Європолу», основний принцип якої полягає в тому, що Партнерські Установи зобов'язуються гарантувати, що вся інформація, яка опрацьовується або проходить через Європол, отримує рівень захисту, еквівалентний тому, який йому надав Європол.

1.2.2. Базові заходи

Система Захисту Європолу SSSR використовується в якості посібника для визначення відповідних заходів контролю для будь-яких систем зв'язку. У принципі, Сторони, що встановили зв'язок між собою, можуть вживати заходи згідно з законодавством кожної Сторони в сфері безпеки задля реагування на загрози, вказані у Системі особливих вимог до захисту (SSSR). Однак, для того, щоб забезпечити мінімальний рівень захисту, нижче перераховані заходи

контролю вважаються основою та передумовою для встановлення мережевого зв'язку.

1.2.2.1. Процедурний контроль

Україна повинна використовувати наступні мінімальні види процедурного контролю:

- Користувачі системи повинні бути відповідним чином перевірені на національному рівні.
- Повинні бути прийняті нормативні правила щодо політики аутентифікації, наприклад, базова інструкція щодо створення та управління паролями.
- Повинні бути прийняті нормативні правила щодо віддаленого доступу до системи та заходів відповідної аутентифікації.
- Повинні бути прийняті нормативні правила щодо ведення облікових записів та аудиту.
- Інформація щодо інцидентів, пов'язаних з питаннями безпеки, які можуть впливати на безпеку мережі Європолу або мережі, яка належить Партнерській Агенції (наприклад, зараження вірусом), повинна бути надана зацікавленим Сторонам у найкоротший термін. Перелік таких інцидентів, пов'язаних з питаннями безпеки, включений в Частину С до цього Додатку.

1.2.2.2. Технічний контроль

Україна повинна використовувати наступні сконфігуровані відповідним чином засоби технічного контролю:

- Граничні пристрої безпеки, такі як міжмережеві екрани або маршрутизатори.
- Антивірусні технології, які підтримують антивірусну політику та стратегії.
- Робочі станції, які безпосередньо підключені до публічних комп'ютерних мереж, таких як Інтернет, не повинні бути підключені або використовуватись для доступу до захищеної мережі Європолу.
- Системи, які опосередковано підключені до публічних комп'ютерних мереж, таких як Інтернет, повинні бути відповідно захищені з метою захисту мережі Європолу від таких публічних мереж.
- Шифрування трафіку при використанні публічних комунікаційних ліній технологіями шифрування повинно відповідати рівню класифікації даних, які захищаються.
- Для гарантування виявлення та усунення вразливості необхідно проводити оцінювання та тестування безпеки інформації.
- Поєднувані системи є суб'єктами системи акредитації (або її еквіваленту).

1.2.2.3. Фізичний контроль

У системах, які підключаються, повинні застосовуватись наступні заходи фізичного контролю:

- Система, яка підключається, повинна бути розташована в захищеному приміщенні.
- Високоточне обладнання, таке як консолі, серверне обладнання, міжмережеві екрани, мережеві комутатори та шифрувальні пристрої, повинне мати контроль фізичного доступу (наприклад, мають бути розміщені в зачиненому приміщенні).

- Доступ до робочих станцій, терміналів тощо, де потенційно існує можливість доступу до Системи Захисту Європолу, повинен бути фізично обмеженим. Там, де необхідно розмістити робочі станції в приміщеннях з публічним доступом з організаційних або оперативних причин, зазначене обладнання повинно бути постійно фізично захищеним від неавторизованого доступу, крадіжки або втрати. Наприклад, таке обладнання не можна залишати без нагляду в публічних місцях.

1.3. Частина C: Приклади інцидентів, що виникають в системі безпеки

Нижче наведено перелік прикладів інцидентів, які можуть генерувати повідомлення про порушення безпеки, і які, як мінімум, повинні розслідуватись та, де це відповідає переліку порушень безпеки, передаватись до Європолу з метою перевірки на виникнення загрози конфіденційності, цілісності та доступу до інформації Європолу.

- Основне джерело струму вимкнуто. З деяких причин джерело безперебійного живлення (UPS) не відповідає вимогам. Всі системи вимкнені.
- Виявлення серйозного вірусу або шкідливого програмного забезпечення.
- Втрата чи викрадення обладнання, яке містить інформацію Європолу або може містити інформацію, використання якої може призвести до несанкціонованого доступу до Системи Захисту Європолу.
- Була здійснена перевірка доступу (також можливе використання системи виявлення вторгнень (IDS). При пошуку по шаблону виявлено, що певний клієнт передає інформацію іншому клієнту (доступ клієнт-клієнт заборонений в системі).
- Журнал подій управління доступом до системи демонструє незвичну активність, наприклад, код доступу працівника часто використовується для входу в приміщення вночі, в той час як зазначений працівник може бути на робочому місці тільки в робочий час – з дев'ятої ранку до п'ятої вечора, і таке перебування не авторизоване.
- Відбулось декілька тривалих атак на головні IP-порти мережевих вузлів.
- Під час поточної перевірки з'ясувалось, що статус звичайного користувача був змінений на статус адміністратора. Працівник зробив це самостійно, підключившись через «Телнет».
- Система не відповідає в звичайний робочий час. При подальшій перевірці адміністратор закриває систему. Метою було встановлення пакету оновлень. Адміністратор забув поінформувати користувачів у встановлений час.
- З'ясовано, що головні IP-порти міжмережевого екрану відкриті, що не було авторизовано відповідною політикою безпеки.
- Будь-який інший інцидент, через який виникає потенційна або реальна загроза інформації Європолу.

1.4. Частина D: Заява про дотримання Кодексу Зв'язку

- Користувачі системи повинні бути відповідним чином перевірені на національному рівні.
- Повинні бути прийняті та впровадженні нормативні правила щодо політики аутентифікації, наприклад, базові інструкції для створення та керування паролями.
- Повинні бути прийняті та впровадженні нормативні правила щодо політики віддаленого доступу та відповідної аутентифікації при підключенні до системи.

- Повинні бути прийняті та впровадженні нормативні правила щодо заходів із ведення облікових записів та аудиту.
- Інформація щодо інцидентів з питань безпеки, які можуть впливати на безпеку мереж Європолу або іншої країни-члена (наприклад, зараження вірусом), повинна передаватись до зацікавленої Сторони якомога швидше.
- Повинні бути встановленими пристрої захисту границь (периметру), такі як міжмережеві екрани або пакетна фільтрація.
- Повинні бути запроваджені такі антивірусні технології, які підтримують антивірусну політику та стратегії.
- Робочі станції, які підключені до публічних комп'ютерних мереж, таких як Інтернет, не можна підключати до захищеної мережі Європолу або використовувати для доступу до Системи Захисту Європолу.
- Системи, які опосередковано підключені до публічних комп'ютерних мереж, таких як Інтернет, повинні бути належним чином захищені з метою захисту Системи Захисту Європолу від зазначених мереж.
- При використанні публічних ліній зв'язку для шифрування трафіку повинні використовуватись криптографічні технології рівня, відповідного до класифікації даних, які захищаються.
- Для гарантування виявлення та усунення вразливості необхідно проводити оцінювання та тестування безпеки інформації.
- Поєднувані системи є суб'єктами системи акредитації (або її еквіваленту).
- Поєднувані системи належним чином розташовані в захищеному місці.
- Високоточне обладнання таке як консолі, серверне обладнання, міжмережеві екрани, мережеві комутатори та шифрувальні пристрої повинні мати контроль фізичного доступу (наприклад, мають бути розміщенні в зачиненому приміщенні).
- Доступ до робочих станцій, терміналів тощо, де потенційно існує можливість доступу до мережі Європолу, повинен бути фізично обмеженим. Там, де необхідно розмістити робочі станції в приміщеннях з публічним доступом з організаційних або оперативних причин, зазначене обладнання повинно бути постійно фізично захищеним від неавторизованого доступу, крадіжки або втрати.

MEMORANDUM OF UNDERSTANDING
on the establishment of a secure communication line between Ukraine and the European Police Office

Ukraine

Represented for the purposes of this Memorandum of Understanding by the Minister of Internal Affairs (hereafter referred to as 'the Ministry'),

and

The European Police Office

Represented for the purposes of this Memorandum of Understanding by the Director (hereafter referred to as 'Europol'),

Hereinafter collectively referred to as the 'Parties' or individually as the 'Party',

Having regard to the Agreement between Ukraine and Europol on strategic cooperation dated 04 December 2009 (hereinafter referred to as "the Agreement on Cooperation"),

Whereas transmission of information between the Parties on the basis of the Agreement on Cooperation requires the establishment of a secure communication line between them,

Whereas the Parties have the intention to further enhance their cooperation by concluding an operational agreement in the future.

Have agreed as follows:

Article 1

Purpose

The purpose of this Memorandum of Understanding is to regulate the procedure of establishment, implementation and operation of a secure communication line for the transmission of information between the Parties.

Article 2

Transmission of information

1. Transmission of information between the Parties shall only take place in accordance with the legislation of Ukraine, Europol's applicable legal framework, and relevant provisions of the Agreement on Cooperation.
2. The transmission of classified information using the secure communication line is limited to the level of RESTREINT UE/EU RESTRICTED and its equivalent in Ukraine.

Article 3

Code of Connection

1. Both Parties undertake to follow minimum standards for security established in Annex 1 to this Memorandum of Understanding (Code of Connection for the Europol Secure Network – hereinafter refereed to as 'Code of Connection'). Both Parties confirm that they have protected the connecting systems to the baseline standards for security with policies and technologies configured appropriately and have considered the controls established in the Code of Connection.
2. By signing this Memorandum of Understanding, the Ministry confirms the Statement of Compliance with the Code of Connection provided in paragraph 1.4 of Part D to the Code of Connection.
3. In the event that one Party substantially deviates from the principles and concepts defined in this Article or in the Code of Connection, the services between the two networks may be terminated until the issues have been resolved.
4. Both Parties agree that if they make an onward interconnection to any other network, then such a connection must be the subject of a similar agreement (Code of Connection) that will stipulate the security baseline.
5. Both Parties agree not to interfere with the ICT equipment of each Party, including (dis)connecting cables or equipment unless specifically instructed or in the case of an emergency.
6. Should a serious security incident occur e.g. a virus infection, it is expected that the Party must consider disconnecting from the other Party's system to protect the further spread of any infection.
7. Before any modifications to networked systems impacting on the other Party's network or the interconnections are implemented, information and sufficient advance notice must be provided in writing to the Head of the Capabilities Department of Europol when the modification impacts Europol and to the respective Contact Point designated for the implementation of this Memorandum of Understanding when the modification impacts the Ministry. Should a meeting be required to discuss the modifications, this should take place prior to any implementation.

8. Both Parties agree to use the interconnected systems only for the purposes established in this Memorandum of Understanding.
9. Each Party is responsible for the security of its own systems from the demarcation point onwards.
10. Both Parties agree not to perform any type of tests, vulnerability scans or intrusions into the others systems without prior authorisation of the other Party.
11. Both Parties agree to share information pertaining to threats and vulnerabilities that may interfere with each others systems.
12. Europol equipment installed on the premises of the Ministry remains the property of Europol. Own equipment of the Ministry installed on the premises of Europol remains the property of the Ministry. The equipment owner is responsible for its security; however bilateral arrangements which deviate from this principle may be made depending on circumstances.
13. Each Party is responsible for the maintenance of its own equipment. Support requests may be made by the system administrators of each Party's respective network, in order to facilitate support and maintenance issues. A procedure to handle such requests will be developed on a bilateral basis between Europol and the Ministry.

Article 4

Purchase, maintenance and distribution of costs

1. In accordance with its procurement rules, Europol shall purchase all goods and services necessary for the establishment, implementation and operation of the secure communication line.
2. The costs of the establishment of the secure communication line shall also be paid by Europol. The secure communication line and all equipment connected to it are supplied by and remain the property of Europol.
3. Europol shall be responsible for maintenance of the secure communication line and, if necessary, for replacement of defective equipment. The Ministry shall, in accordance with the applicable procedures, provide access for any personnel designated by Europol for such maintenance and replacement of defective equipment to the relevant areas of its premises. In case a malfunction is detected by the Ministry, Europol User Support personnel shall be the first line of technical assistance.
4. The monthly running costs for the secure communication line shall be shared between the Parties with each paying 50%. Europol will pay in advance all the monthly running costs as necessary. The Ministry will reimburse 50% of the monthly running costs, as actually incurred, following a recovery order issued by Europol on a quarterly basis, in accordance with the Europol Financial Regulation.
5. Should the secure communication line be dismantled, the Ministry shall transfer to Europol the items registered as Europol's assets. Europol shall transfer to the Ministry the items registered as Ministry's assets.
6. All imports by and, where applicable, all exports from Europol shall be allowed to enter or to leave Ukraine without being subject to customs, import or export duties, charges, levies, Value Added Tax (VAT) or to any other duties, charges, levies and taxes of equivalent effect. Such exemption shall only be applied to the imports or exports in connection with the goods or equipment supplied or to be shipped back and/or services rendered by Europol under this Memorandum of Understanding.

Article 5

Liability and settlement of disputes

1. Without prejudice to Article 13 of the Agreement on Cooperation, a Party shall be liable for damage caused to the other Party as a result of the establishment, the implementation or the operation of the secure communication line. In such cases, the Parties shall endeavour to find an equitable solution for the compensation of damages suffered.
2. Any dispute between the Parties concerning the interpretation or application of this Memorandum of Understanding shall be settled in accordance with Article 14 of the Agreement on Cooperation.

Article 6

Amendments

Amendments to this Memorandum of Understanding shall be mutually agreed upon in writing between the Parties.

Article 7

Termination

This Memorandum of Understanding may be terminated in writing by either of the Parties with three months' notice.

Article 8

Entry into force and signatures

This Memorandum of Understanding shall enter into force on the date on which Ukraine notifies Europol, in writing, through diplomatic channels, that it has completed its internal procedures necessary for the entry into force of the Memorandum of Understanding.

This Memorandum of Understanding is concluded in the Ukrainian and English languages, each text being equally authentic. In case of divergences in interpretation, the English version shall prevail. Signed in duplicate.

Kiev

Signed on 11.03.2015

For Ukraine

Mr. Arsen AVAKOV

Minister

The Hague,

Signed on 19/3/15

For Europol

Mr. Rob Wainright

Director

1. Annex 1: Code Of Connection

1.1. Part A: Introduction

The primary purpose of this Code of Connection (CoCo) is to provide assurance that the Europol Secure Network and the external networks (Partner Agencies) that are interconnected to it are adequately protected against threats to confidentiality, integrity and availability. It is acknowledged that a security incident in the network of one Partner Agency or Europol could potentially affect the interconnected networks of all other Partner Agencies.

The key principle of this Code of Connection is that all Partner Agencies connected to the Europol Secure Network need to implement a minimum set of security controls. This security baseline will aim at reducing the risk of security incidents occurring anywhere in the interconnected system from impacting the security of the entire network down to a level acceptable to the Security Accreditation Authority. Each Partner Agency is responsible for the security of its own systems from the demarcation point onwards.

The Code of Connection is binding upon Europol and the Partner Agency. The concepts, principles, controls and obligations mentioned therein shall be complied with and respected.

1.2. Part B: Minimum Security Controls

1.2.1. Europol Secure Network System Specific Security Requirements

Europol maintains a list of network infrastructure security requirements in a document entitled "Europol Secure Network System Specific Security Requirements (SSSR), File No. 2440-72". An SSSR is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met by a system. It is based on the key security principles established by the Europol Security Manual and the result of the risk assessment.

The Europol Secure Network SSSR was adopted by the Management Board on the recommendation of the Europol Security Committee. This document is subject to regular review and updating in the context of the re-accreditation of the system.

A mandatory requirement for interconnection of an external network to the Europol Secure Network is that Ukraine and Europol must implement policies, procedures and technical measures that are comparable to those mentioned in the SSSR document. That is not to say that the actual procedures or technicalities must be the same, simply that the concepts mentioned within the SSSR must be addressed according to national policies and guidelines. This is in line with article 2 of the Rules on confidentiality of Europol information, in which the principle is established that Partner Agencies undertake to ensure that all information which is processed by or through Europol shall receive a level of protection which is equivalent to the protection afforded by Europol to such information.

1.2.2. Baseline Measures

The Europol Secure Network SSSR should be used as a guide to define control measures for any interconnected system. In principle, connecting Parties may choose to implement the measures which are appropriate in accordance with

local security policies and regulations to address the threats and concepts mentioned in the SSSR. However, in order to ensure a minimum level of security assurance, the control measures listed below are a baseline and a prerequisite to a network interconnection.

1.2.2.1. Procedural Controls

Ukraine must employ the following minimum procedural controls:

- Users of the system must be security cleared to the appropriate national level.
- An authentication policy, i.e. baseline guidelines for password construction and management, must be in place.
- A policy for any remote access and appropriate authentication measures to the connecting system should be in place.
- Accounting and audit measures for the connecting system must be in place.
- Information relating to security incidents that have the potential to interfere with the security of Europol's or the interconnected network of a Partner Agency (such as a virus infection) should be reported to any concerned Parties as soon as possible. A list of such security incidents is included in Part C to this Annex.

1.2.2.2. Technical Controls

Ukraine must employ the following appropriately configured technical controls:

- Boundary (perimeter) security devices such as firewalls or screening routers.
- Anti virus technologies supported by an anti virus policy and strategy.
- No workstation directly connected to a public computer network such as the Internet may be connected to the Europol Secure Network or used to access the Europol Secure Network.
- Systems that are indirectly connected to a public network such as the Internet must be appropriately protected in order to protect the Europol Secure Network from such a public network.
- Encryption of traffic when public communications lines are used, such as encryption technology, must be of an appropriate strength for the classification of data that it is intended to protect.
- Information security assessments and tests are carried out to ensure that vulnerabilities are identified and remediated.
- Connecting systems are subject to an accreditation (or equivalent) regime.

1.2.2.3. Physical Controls

Connecting systems must employ the following physical controls:

- The connecting system must be appropriately located in a secure location.
- Sensitive equipment such as consoles, server equipment, firewalls, network switches and encryption devices must employ physical access control (e.g. located in a locked room).
- Access to workstations, terminals etc, where potential to access the Europol Secure Network exists must be physically restricted. Where

workstations need to be located in a publicly accessible area for organisational or operational reasons, such equipment must be physically protected at all times from unauthorised access, theft or loss. For example, such equipment must not be left unattended in public places.

1.3. Part C: Examples of Security Incidents

The following is a list of examples that may generate a security alert, as a minimum they should be investigated, and, where appropriate, notified to Europol to check that no threat to the confidentiality, integrity or availability of Europol information has taken or could have taken place.

- The main power goes down. For some reason the UPS does not respond. All systems are down.
- A serious virus or other malware incident.
- Loss or theft of equipment that contains Europol information or may contain information that could lead to unauthorised access to the Europol Secure Network.
- A log-check is done (it could also be the use of an IDS). When looking for certain patterns, it becomes clear that a normal client is distributing information to another client (client-to-client access is not allowed in the system).
- The log of the access control system shows unusual activity e.g. a staff member's coded pass is used frequently for entering the building at night when the actual coded pass holder should only be working nine-to-five and this activity had not been authorised.
- There have been several sustained attacks on key IP ports of network hosts.
- At a routine check it appears that a normal user has been changed to administrator. The person did it himself by logging on with Telnet.
- A system is not responding during normal working hours. When checking further, an administrator closed the system. The purpose was to install a service pack. He forgot to inform the users in due time.
- Key IP Ports in the firewall are found open, which have not been previously authorised by the relevant security policy.
- Any other incident whereby there is a potential or actual threat to Europol information.

1.4. Part D: Statement of Compliance to the Code of Connection

- Users of the system are security cleared to the appropriate national level.
- An authentication policy, i.e. baseline guidelines for password construction and management, is in place and implemented.
- A policy for any remote access and appropriate authentication measures to the connecting system is in place and implemented.
- Accounting and audit measures for the connecting systems are in place and implemented.
- Information relating to security incidents that have the potential to interfere with the security of Europol's or another Member States Network (such as a virus infection) is reported to any concerned Parties as soon as possible.

- Boundary (perimeter) security devices such as firewalls or screening routers are implemented.
- Anti virus technologies supported by an anti virus policy and strategy are implemented.
- No workstation directly connected to a public computer network such as the Internet are connected to the Europol Secure Network or used to access the Europol Secure Network.
- Systems that are indirectly connected to a public network such as the Internet are appropriately protected in order to protect the Europol Secure Network from such a public network.
- Encryption of traffic when public communications lines are used, such as encryption technology, must be of an appropriate strength for the classification of data that it is intended to protect.
- Information security assessments and tests are carried out to ensure that vulnerabilities are identified and remediated.
- Connecting systems are subject to an Accreditation (or equivalent) regime.
- The connecting systems are appropriately located in a secure location.
- Sensitive equipment such as consoles, server equipment, firewalls, network switches and encryption devices employ physical access control (e.g. located in a locked room).
- Access to workstations, terminals etc, where potential to access the Europol network exists must be physically restricted. Where workstations need to be located in a publicly accessible area for organisational or operational reasons, such equipment must be physically protected at all times from unauthorised access, theft or loss.

«ЗАТВЕРДЖУЮ»

«1» квітня 2015 року

В.О.Шкілевич

Т.в.о. Директора

Департаменту міжнародного права

МЗС України

№ 72/14-612-739 від «1» квітня 2015 року.

Я, Павлишин О.Я., начальник відділу міжнародних договорів та офіційних перекладів Департаменту міжнародного права МЗС України, засвідчую вірність копії Меморандуму про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку, вчиненого 11 березня 2015 року в м. Київ та 19 березня 2015 року в м. Гаага українською та англійською мовами.

Документ на 16 арк.

Підпис: