



НАЦІОНАЛЬНЕ АНТИКОРУПЦІЙНЕ БЮРО УКРАЇНИ

НАКАЗ

«__» _____ 20__ року

№ _____

Про введення в дослідну експлуатацію системи безпечного обміну даними, побудованої на базі програмного забезпечення ProjectSend, та затвердження Тимчасового положення про її використання у Національному антикорупційному бюро

З метою організації захищеного та контрольованого обміну документами і матеріалами з Офісом Генерального прокурора, Міністерством юстиції України та правоохоронними органами іноземних держав у рамках міжнародного співробітництва, з метою встановлення єдиних вимог до використання системи безпечного обміну даними, побудованої на базі програмного забезпечення ProjectSend, керуючись пунктом 5 частини першої статті 8 Закону України «Про Національне антикорупційне бюро України»,

НАКАЗУЮ:

1. Ввести в дослідну експлуатацію систему безпечного обміну даними, побудованої на базі програмного забезпечення ProjectSend (далі – Система), у Національному антикорупційному бюро України (далі – Національне бюро).

2. Затвердити Тимчасове положення про використання Системи у Національному бюро (далі – Положення), що додається.

3. Підрозділу детективів кримінального аналізу (Лобач І.А.):
забезпечити адміністрування Системи та усунення недоліків, виявлених у процесі її дослідної експлуатації;

надати Управлінню інформаційних технологій перелік віртуальних серверів, які входять до складу Системи, та пропозиції щодо внесення змін до Переліку інформаційних активів, що підлягають резервному копіюванню в частині баз даних, конфігураційних файлів (налаштувань), компонентів програмного забезпечення, журналів подій тощо;

розробити плани резервного копіювання та зберігання інформаційних активів, плани відновлення інформаційних активів, графік перевірки резервних копій.



4. Підрозділу детективів інформаційної безпеки (Журавльов Ю.В.) забезпечити здійснення заходів з інформаційної безпеки та захисту інформації у Системі відповідно до встановлених вимог захисту інформації.

5. Управлінню інформаційних технологій (Морозов О.В.):
забезпечити резервування віртуальних серверів Системи;
внести під час наступного щорічного оновлення зміни до Переліку інформаційних активів, що підлягають резервному копіюванню, в частині, що стосується Системи.

6. Відділу по роботі з медіа (Живага М.С.) оприлюднити цей наказ на офіційному вебсайті Національного бюро.

7. Відділу документообігу (Асанова Л.М.) ознайомити з цим наказом Першого заступника Директора Національного бюро, заступників Директора Національного бюро, заступника Директора Національного бюро з питань цифрового розвитку та цифрових трансформацій, керівників головних підрозділів детективів, Підрозділу детективів з фінансових розслідувань, Другого Головного спеціального підрозділу детективів (Д-2), Підрозділу детективів організаційно-аналітичного забезпечення та стратегічного розвитку, Підрозділу детективів інформаційної безпеки, Підрозділу детективів О-2, Управління внутрішнього контролю, Управління інформаційних технологій та Підрозділу детективів кримінального аналізу.

8. Контроль за виконанням цього наказу залишаю за собою.

Директор

Семен КРИВОНОС

ЗАТВЕРДЖЕНО

Наказ Національного
антикорупційного бюро України
«___»_____ 2026 р. №_____

ТИМЧАСОВЕ ПОЛОЖЕННЯ **про використання системи безпечного обміну даними,** **побудованої на базі програмного забезпечення ProjectSend,** **у Національному антикорупційному бюро України**

I. Загальні положення

1. Це Тимчасове положення визначає загальні правила використання на час дослідної експлуатації системи безпечного обміну файлами, побудованої на базі програмного забезпечення ProjectSend (далі – Система), у Національному антикорупційному бюро України (далі – Національне бюро) як платформи для організації захищеного та контрольованого обміну файлами з Офісом Генерального прокурора, Міністерством юстиції України та правоохоронними органами іноземних держав у рамках міжнародного співробітництва.

2. Використання Системи здійснюється з дотриманням вимог нормативно-правових актів та інших документів Національного бюро з питань інформаційної безпеки, режиму доступу та захисту інформації.

3. Забороняється обробляти в Системі інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законодавством.

4. Технічні налаштування сервера, політик безпеки, журналювання та засобів адміністрування визначаються внутрішніми процедурами та/або політиками з урахуванням вимог інформаційної безпеки.

5. Відхилення від вимог цього Положення допускаються виключно за наявності резолюції Директора до службової записки, погодженої з Підрозділом детективів інформаційної безпеки та Управлінням внутрішнього контролю.

II. Терміни

1. У цьому Положенні наведені нижче терміни мають таке значення:

ProjectSend – програмне забезпечення з відкритим вихідним кодом, розгорнуте на віртуальному сервері Національного бюро та призначене для організації захищеного та контрольованого обміну файлами з Офісом Генерального прокурора, Міністерством юстиції України та правоохоронними органами іноземних держав у рамках міжнародного співробітництва;

адміністрування Системи – сукупність технічних дій з налаштування, підтримки та забезпечення працездатності Системи, які не включають функції контролю за дотриманням вимог захисту інформації;

журналювання – автоматизована реєстрація та збереження відомостей про події, дії користувачів і адміністраторів у Системі;

інцидент інформаційної безпеки – подія або сукупність подій, що призвели або можуть призвести до порушення конфіденційності, цілісності чи доступності інформації в Системі;

компрометація облікового запису – отримання або ймовірне отримання сторонньою особою несанкціонованого доступу до облікового запису користувача чи адміністратора;

користувачі Системи – посадові особи, які мають обліковий запис у Системі та здійснюють у ній визначені цим Положенням дії відповідно до наданих прав доступу (адміністратор Системи, менеджери, клієнти);

мінімально необхідний доступ – надання користувачу менеджеру та адміністратору лише тих прав доступу, які потрібні для виконання посадових функцій та обов’язків, на мінімально необхідний строк і щодо мінімального кола папок та файлів;

обліковий запис – сукупність облікових даних (логін, пароль та за потреби додаткові засоби автентифікації), що ідентифікують користувача в Системі та визначають надані йому права доступу;

2. Інші терміни вживаються у значеннях, визначених Законом України «Про захист інформації в інформаційно-комунікаційних системах», іншими актами законодавства України та актами Національного бюро.

III. Суб’єкти використання Системи

1. Суб’єктами використання Системи є суперадмін, адміністратор безпеки, адміністратор Системи, менеджери, клієнти.

2. Розподіл суб’єктів за наявністю облікового запису в Системі та основними функціями здійснюється таким чином:

Суб’єкт	Наявність доступу до Системи	Основна функція
Суперадмін	Окремий обліковий запис з максимальним рівнем технічних прав; використовується виключно на етапі первинного розгортання (налаштування) Системи	Первинне технічне розгортання Системи, створення облікового запису адміністратора Системи
Адміністратор безпеки	Обліковий запис з роллю мінімального перегляду, без права внесення змін та доступу до вмісту файлів;	Контроль захисту інформації, реагування на інциденти

Суб'єкт	Наявність доступу до Системи	Основна функція
	здійснює моніторинг подій інформаційної безпеки	
Адміністратор системи	Обліковий запис з правами технічного адміністрування, без права доступу до вмісту файлів, розміщених у Системі	Технічне адміністрування Системи (управління обліковими записами, конфігурацією тощо)
Менеджер	Обліковий запис з правами управління файлами та клієнтами	Організація обміну файлами в Системі
Клієнт	Обліковий запис з обмеженими правами	Завантаження/отримання файлів у межах наданого доступу

3. Особи, які виконують функції суперадміна, Адміністратора безпеки, адміністратора Системи та перелік менеджерів визначається окремим наказом Директора Національного бюро, або особи, яка виконує обов'язки Директора Національного бюро.

4. Суперадмін – окремий обліковий запис з максимальним рівнем технічних прав доступу до Системи, включно з правом створення, зміни та видалення облікового запису адміністратора Системи. Функції суперадміна виконує посадова особа відділу детективів з цифрових розслідувань та управління кримінальними даними Підрозділу детективів кримінального аналізу під окремим обліковим записом, відмінного від облікового запису адміністратора Системи. Обліковий запис суперадміна використовується виключно на етапі первинного розгортання (налаштування) Системи для створення облікового запису адміністратора Системи. Після створення облікового запису адміністратора Системи обліковий запис суперадміна залишається активним, проте не використовується для виконання поточних завдань адміністрування Системи, у тому числі для доступу до вмісту файлів, розміщених у Системі.

5. Адміністратор безпеки – посадова особа Підрозділу детективів інформаційної безпеки Національного бюро, яка здійснює контроль за дотриманням вимог щодо захисту інформації в Системі. Адміністратору безпеки надається обліковий запис з роллю, що передбачає виключно перегляд журналу активності Системи та іншої службової інформації в обсязі, необхідному для виконання функцій контролю, без права внесення змін до налаштувань Системи, керування обліковими записами користувачів та без доступу до вмісту файлів, розміщених у Системі. Створення такого облікового запису та визначення параметрів відповідної ролі забезпечується адміністратором Системи.

6. Адміністратор Системи – посадова особа відділу детективів з цифрових розслідувань та управління кримінальними даними Підрозділу детективів кримінального аналізу, яка здійснює технічне адміністрування Системи. Адміністратору Системи надається обліковий запис з правами технічного адміністрування, необхідним для забезпечення функціонування Системи (зокрема, управління обліковими записами користувачів Системи, налаштування конфігурації), без права доступу до вмісту (перегляду, завантаження) файлів, розміщених користувачами в Системі.

7. Менеджери – посадові особи Міжнародно-правового відділу Національного бюро, яким надано обліковий запис в Системі для організації обміну файлами з клієнтами.

8. Клієнт – користувач, якому на визначений строк надано обліковий запис в Системі для завантаження та/або отримання файлів у межах взаємодії з Національним бюро.

IV. Загальні правила використання сервісу

1. Система використовується виключно через персональний обліковий запис. Робота під іншим обліковим записом забороняється. Передача власних облікових даних іншим особам, у тому числі іншим суб'єктам використання Системи, забороняється.

2. Перед завантаженням файлу до Системи користувач Системи зобов'язаний самостійно перевірити, чи існує у відповідній папці/розділі файл з ідентичною або подібною назвою.

3. Завантаження файлів до Системи здійснюється менеджером до розділу, закріпленого за відповідним клієнтом. Клієнт має доступ тільки до розділу, закріпленого за ним, у межах якого може переглядати та завантажувати файли, розміщені менеджером, а також надавати (завантажувати) власні файли до Системи.

4. У Систему завантажуються виключно файли, необхідні для виконання службових завдань. Зберігання особистих матеріалів, не пов'язаних із діяльністю Національного бюро, забороняється.

5. У назвах файлів і папок забороняється зазначати відомості, що можуть розкривати зміст документів, а також паролі, ключі або інші облікові дані. У разі завантаження нової версії документа користувач Системи зобов'язаний присвоїти файлу назву, що відрізняється від назви попереднього файлу (шляхом додавання дати у форматі ДД-ММ-РРРР та/або номера версії).

6. Для кожного файлу, що завантажується до Системи, користувач Системи зазначає термін дії (expiry date) у відповідному полі за допомогою функціоналу ProjectSend. Строк зберігання файлу, встановлений користувачем Системи, не може перевищувати 7 днів з моменту завантаження. У разі необхідності зберігання файлу довше цього строку користувач до його спливу повторно завантажує файл із зазначенням нового строку дії.

7. Менеджер, відповідальний за папку, зобов'язаний своєчасно вживати заходів щодо видалення неактуальних (застарілих, дубльованих, відкликаних) файлів. Накопичення застарілих версій не допускається.

Менеджер видаляє неактуальні файли самостійно, в межах закріплених за ним папок/клієнтів.

Клієнт має право самостійно видаляти лише ті файли, які він власноруч завантажив до Системи.

8. Забороняється вивантажувати файли з Системи до зовнішніх або хмарних сервісів, особистих пристроїв, месенджерів та інших неконтрольованих ресурсів, якщо це не погоджено з Підрозділом детективів інформаційної безпеки.

9. У разі помилкового видалення файлу користувач Системи невідкладно, але не пізніше одного робочого дня з моменту виявлення, звертається до адміністратора Системи із заявкою на відновлення файлу. Адміністратор Системи протягом одного робочого дня з моменту отримання заявки перевіряє факт та обставини видалення файлу і, за наявності підстав, звертається до Управління інформаційних технологій із запитом на розгортання копій віртуальних серверів Системи. Управління інформаційних технологій на підставі отриманого запиту розгортає відповідні копії віртуальних серверів Системи в ізолюваному відновлювальному середовищі у строк не пізніше наступного робочого дня з моменту отримання запиту. Пошук та ідентифікація потрібного файлу в розгорнутій копії здійснює користувач Системи спільно з адміністратором Системи. Ідентифікований файл передається адміністратору Системи, який здійснює його повторне завантаження у робочу версію Системи засобами стандартного функціоналу завантаження файлів ProjectSend. Після завершення робіт з відновлення файлу Управління інформаційних технологій видаляє розгорнуту копію з відновлювального середовища.

10. Файли, розміщені в Системі у зв'язку з виконанням службових повноважень, є інформаційними ресурсами Національного бюро, незалежно від того, ким саме вони були завантажені.

11. Система призначена для обміну файлами між користувачами в установленому цим Положенням порядку.

V. Права, обов'язки та заборони суб'єктів використання Системи

1. Права адміністратора безпеки:

1) надавати адміністратору Системи обов'язкові до виконання приписи щодо усунення виявлених порушень і недоліків захисту інформації;

2) ініціювати перед Керівництвом Національного бюро питання про обмеження чи припинення доступу користувача в разі виявлення порушень або загрози безпеці інформації.

2. Обов'язки адміністратора безпеки:

1) виявляти ознаки та реагувати на інциденти інформаційної безпеки, пов'язані з Системою;

2) інформувати керівництво Національного бюро та Управління внутрішнього контролю про стан захищеності Системи та про виявлені інциденти.

Адміністратор безпеки є координатором реагування на інциденти інформаційної безпеки, пов'язані з Системою.

3. Права адміністратора Системи:

1) Створювати змінювати та припиняти дію облікових записів менеджерів, надавати змінювати та припиняти дію ролей (прав доступу) облікових записів клієнтів;

2) визначати технічні параметри роботи Системи у межах, що не суперечать вимогам захисту інформації.

4. Обов'язки адміністратора Системи:

1) здійснювати адміністрування Системи в повному обсязі, наданому обліковим записом;

2) забезпечувати технічну працездатність Системи, її оновлення;

3) попередньо погоджувати з адміністратором безпеки будь-які зміни налаштувань Системи, що впливають на рівень її захищеності, та вносити такі зміни лише після отримання такого погодження;

4) виконувати приписи адміністратора безпеки щодо усунення порушень і недоліків захисту інформації;

5) невідкладно інформувати адміністратора безпеки про виявлені інциденти інформаційної безпеки або про події, що можуть свідчити про їх виникнення.

5. Права Менеджера:

1) здійснювати розподіл файлів за категоріями/групами в межах Системи;

2) створювати та припиняти (блокувати) облікові записи клієнтів.

3) надавати клієнтам доступ до визначених файлів у межах наданих менеджеру прав;

6. Обов'язки менеджера:

1) контролювати своєчасність та коректність обміну файлами з клієнтами;

2) невідкладно, але не пізніше одного робочого дня з моменту, коли менеджеру стало відомо про завершення взаємодії з клієнтом, зміну відповідальної особи клієнта або настання інших обставин, що впливають на необхідність доступу клієнта до Системи, здійснювати припинення (блокування) дії облікового запису такого клієнта;

3) невідкладно інформувати адміністратора безпеки та адміністратора системи про виявлені інциденти інформаційної безпеки або про події, що можуть свідчити про їх виникнення.

7. Права клієнта:

1) здійснювати завантаження та/або перегляд файлів у межах наданих йому прав доступу;

2) отримувати сповіщення, передбачені функціоналом Системи, щодо доступних йому файлів.

8. Обов'язки клієнта:

1) забезпечувати конфіденційність своїх облікових даних;

2) невідкладно повідомляти менеджера та адміністратора безпеки про виявлені інциденти інформаційної безпеки або про події, що можуть свідчити про їх виникнення.

9. Повідомлення про виявлені інциденти або події, що можуть свідчити про їх виникнення, невідкладно повідомляють: клієнт – менеджера та адміністратора безпеки; менеджер – адміністратора безпеки та адміністратора Системи; адміністратор Системи – адміністратора безпеки. Адміністратор безпеки забезпечує координацію реагування на такі повідомлення відповідними підрозділами Національного бюро.

VI. Порядок надання, зміни та припинення доступу

1. Підставою для створення облікового запису менеджера є наказ Директора Національного бюро, або особи, яка виконує обов'язки Директора Національного бюро.

2. Підставою для створення облікового запису клієнта є звернення (у тому числі електронне) органу, представником якого є клієнт, або ініціатива працівника Міжнародно-правового відділу, відповідального за взаємодію з таким клієнтом. Рішення про створення облікового запису клієнта приймається начальником Міжнародно-правового відділу Національного бюро.

3. Обліковий запис менеджера створюється адміністратором Системи, який надає менеджеру права доступу для виконання службових обов'язків на підставі, визначеній пунктом 1 цього розділу.

4. Обліковий запис клієнта створюється та припиняється (блокується) менеджером самостійно, без залучення адміністратора Системи. Строк дії облікового запису клієнта визначається менеджером з урахуванням мети та строку взаємодії з клієнтом (зокрема, строку виконання відповідного доручення, міжнародного співробітництва тощо) і не може перевищувати 12 місяців. У разі необхідності продовження строку дії облікового запису клієнта менеджер до закінчення поточного строку самостійно продовжує строк дії такого облікового запису на новий строк, що не може перевищувати 12 місяців.

5. Менеджер надає доступ до визначених файлів визначеному клієнту.

6. У разі зміни функціональних обов'язків менеджера або припинення трудових відносин з ним, начальник Міжнародно-правового відділу (або особа, яка виконує обов'язки начальника Міжнародно-правового відділу) зобов'язаний невідкладно, але не пізніше одного робочого дня, проінформувати адміністратора Системи про необхідність зміни або припинення дії облікового запису менеджера.

7. Адміністратор Системи зобов'язаний невідкладно, але не пізніше 24 годин після отримання повідомлення, виконати відповідні дії.

8. У разі звільнення працівника, який є клієнтом в Системі, зміни відповідальної особи або настання інших обставин, що впливають на необхідність доступу працівника до Системи, клієнт повідомляє про це відповідного менеджера наявними каналами зв'язку.

9. Міжнародно-правовий відділ Національного бюро не рідше одного разу на квартал звертається до уповноважених представників клієнтів Системи з метою уточнення актуальності інформації щодо осіб, яким необхідний доступ до Системи, зокрема у разі їх звільнення, зміни відповідальної особи або виникнення інших обставин, що впливають на необхідність такого доступу. У разі виявлення обставин, що впливають на необхідність доступу клієнта, відповідний менеджер невідкладно, але не пізніше одного робочого дня, здійснює відповідне припинення (блокування) облікового запису такого клієнта.

10. Перегляд наданих користувачам Системи прав доступу здійснюється адміністратором Системи на регулярній основі, не рідше одного разу на квартал, з метою підтвердження відповідності обсягу наданих прав доступу мінімально необхідному доступу та фактичними службовими потребами користувача, а також з метою виявлення облікових записів клієнтів, строк дії яких сплив.

11. Обліковий запис адміністратора Системи використовується для здійснення адміністративних функцій та передбачає надання розширених прав доступу до Системи. Надання зміна та припинення таких прав доступу здійснюється на підставі наказу Директора Національного бюро, або особи, яка виконує обов'язки Директора Національного бюро. Контроль за використанням розширених прав доступу адміністратора Системи здійснюється адміністратором безпеки в порядку, визначеному пунктом 5 розділу III цього Положення.

VII. Адміністрування, моніторинг і журналювання

1. Адміністрування Системи здійснюється адміністратором Системи у межах службових обов'язків та повноважень, визначених цим Положенням.

2. Журнали активності Системи передаються до централізованого засобу збирання, зберігання та аналізу подій інформаційної безпеки (SIEM). Адміністратор Системи забезпечує технічне передавання журналів, а адміністратор безпеки – їх моніторинг та аналіз.

3. В Системі має здійснюватися журналювання подій, пов'язаних із:

- входом до облікових записів;
- завантаженням, вивантаженням, переміщенням або видаленням файлів;
- створенням, зміною або видаленням папок та проєктів;
- наданням, зміною або припиненням доступу;
- адміністративними діями.

4. Моніторинг подій інформаційної безпеки здійснюється адміністратором безпеки самостійно у межах доступу, без додаткового звернення до адміністратора Системи.

Журнали активності зберігаються в Системі не менше 3 років.

Адміністратор Системи надає журнали активності та відомості про дії конкретного користувача Управлінню внутрішнього контролю на підставі його письмового запиту, підписаного керівником Управління внутрішнього контролю (або особою, яка виконує обов'язки керівника Управління внутрішнього

контролю), без необхідності отримання резолюції Директора Національного бюро. Відповідальність за відповідність запиту функціям Управління внутрішнього контролю покладається на Управління внутрішнього контролю.

Адміністратор Системи надає журнали активності та відомості про дії конкретного користувача Підрозділу детективів інформаційної безпеки на підставі службової записки керівника зазначеного підрозділу, погодженої Управлінням внутрішнього контролю.

VIII. Відповідальність

1. Користувачі Системи несуть персональну відповідальність за дії, виконані під їх обліковим записом, якщо не встановлено обставин компрометації або інших подій, що не залежали від користувача.

2. Адміністратор Системи несе відповідальність за належне виконання адміністративних дій у межах наданих повноважень, а також за розголошення відомостей, отриманих під час адміністрування, згідно з чинним законодавством України.

3. Адміністратор безпеки несе відповідальність за несвоєчасне виявлення інцидентів інформаційної безпеки, пов'язаних із Системою, або нереагування на них, а також за розголошення відомостей, що стали йому відомі у зв'язку з виконанням покладених на нього функцій, згідно з чинним законодавством України.

4. Відповідальність за зміст завантажених файлів та коректність вибору папки для їх розміщення несе користувач, який здійснив завантаження.

5. Порушення вимог цього Положення можуть бути підставою для юридичної відповідальності.

Т.в.о. Керівника Підрозділу
детективів кримінального аналізу

Ілля ЛОБАЧ