Додаток № 1
до Договору про надання доступу
до Інформаційної
системи портового співтовариства
від «___» _____ 2014 року

Інструкція користувачу
автоматизованої системи класу «3» єдиної інформаційної системи портового співтовариства
(інформаційної системи портового співтовариства)

1. Електронно-обчислювальні машини (ЕОМ), які використовуються для обробки конфіденційної інформації, відноситься до об'єктів електронно-обчислювальної техніки (ЕОТ).

2. Для забезпечення необхідного рівня захисту конфіденційної інформації від несанкціонованого доступу (НСД) в автоматизованій системі (АС)використовуються організаційно-технічні заходи.

3. Носії, які призначені для роботи з конфіденційною інформацією в АС та носії ключової інформації повинні бути зареєстровані у "Журналі обліку магнітних носіїв інформації" і зберігатися у сховищах, які призначені для збереження документів, справ, видань та інших матеріальних носіїв конфіденційної інформації. На них розповсюджуються такі ж правила, які діють для паперових документів з відповідним грифом.

4. Порядок обробки в АС документів, які містять конфіденційну інформацію, розроблено відповідно до таких документів:

– Перелік відомостей, що становлять конфіденційну інформацію в товаристві з обмеженою відповідальністю "ППЛ 33-35";

– Інструкція про порядок обліку, зберігання, використання, та знищення носіїв конфіденційної інформації в ТОВ «ППЛ 33-35».

5. Перед початком роботи в АС користувач зобов'язаний:

– Мати особистий ключ, отриманий від Центру сертифікації ключів у встановленому порядку. Перелік необхідних документів для отримання ЕЦП розміщений на веб-сторінці ЦСК.

– Ознайомитись в частині, що його стосується, з організаційно-технічними документами, які регламентують правила обробки конфіденційної інформації в АС. Дозволяється ознайомлення користувача з необхідними документами в електронному вигляді.

– Мати встановлену на ЕОМ Клієнтську частину програмного забезпечення єдиної інформаційної системи портового співтовариства.

Клієнтська частина програмного забезпечення єдиної інформаційної системи портового співтовариства (далі – ПЗ) може бути встановлена на ЕОМ, яка відповідає наступним вимогам:

- на ЕОМ встановлена ліцензійна версія операційної системи (ОС) Windows XP Professional Service Pack 2 або більш новітньої версії;

- настроювання параметрів безпеки ОС проведене у відповідності до Інструкції з інсталяції та конфігурування параметрів безпеки для відповідної операційної системи;

- на ЕОМ встановлене ліцензійне антивірусне програмне забезпечення з переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України. Вказаний перелік розміщений на веб-сторінці Державної служби спеціального зв'язку та захисту інформації України (**http://dstszi.kmu.gov.ua** *Діяльність » Експертиза » Технічний захист інформації » Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації*). Антивірусні бази повинні регулярно оновлюватись.

– Обов'язково повинен бути встановлений пароль на завантаження ЕОМ.

6. В процесі роботи в АС користувач зобов'язаний:

– Дотримуватися встановлених вимог нормативних документів щодо роботи з конфіденційною інформацією. Користувачі несуть особисту відповідальність за дотримання ними встановлених правил обробки конфіденційної інформації під час роботи в АС.

– Спостерігати, щоб дані, які виводяться на екран монітору не були доступні для спостереження іншим особам.

– Дотримуватися Регламенту ЦСК та Договору про надання послуг ЕЦП.

7. Користувачеві категорично заборонено:

– Проводити роботи з обробки конфіденційної інформації без виконання всіх заходів щодо захисту інформації.

– Обробляти конфіденційну інформацію при виявленні будь-яких несправностей або збоїв у роботі програмного та апаратного забезпечення.

– Декомпілювати ПЗ або вносити будь-які зміни в файли ПЗ.

– Розголошувати відомості щодо заходів захисту від несанкціонованого доступу.

– Встановлювати будь-яке неліцензійне або стороннє програмне забезпечення, яке може спричинити виток конфіденційної інформації, тобто комп'ютерних вірусів, клавіатурних шпигунів тощо.

– Обробляти конфіденційну інформацію під час знаходження у приміщенні сторонніх осіб.

– Під час обробки конфіденційної інформації залишати робоче місце.

– Використовувати для роботи з конфіденційною інформацією змінні носії (дискети, оптичні диски, flash-пам'яті тощо), які не пройшли відповідну реєстрацію.

– Залишати без нагляду та передавати іншим особам отримані змінні носії.

8. Правила використання ключа ЕЦП і пароля доступу до ключа:

– Носії з ключами ЕЦП реєструються в журналі за місцем роботи користувача.

– Після завершення роботи в АС завжди відключайте носій з ключем ЕЦП.

– У разі виникнення підозр на компрометацію ключа ЕЦП (копіювання чи втрата носія, порушення правил зберігання особистих ключів, виникнення підозр на несанкціоноване застосування особистого ключа, втрата контролю щодо особистого ключа через компрометацію коду доступу до носія особистого ключа, випадки, коли не можна вірогідно встановити, що відбулося з носієм, що містить ключову інформацію, наприклад, коли носій вийшов з ладу й доказово не спростована можливість того, що даний факт відбувся в результаті несанкціонованих дій зловмисника) або компрометацію середовища виконання (наявність в комп'ютері програм-шпигунів) його власник повинен негайно повідомити про це співробітника Акредитованого центра сертифікації ключів (АЦСК) та вжити заходів щодо скасування відповідного сертифікату відкритого ключа.

– У разі крадіжки ключа ЕЦП зміна пароля доступу до ключа ЕЦП не захищає від використання його зловмисниками. З метою дотримання безпеки необхідно заблокувати ключ ЕЦП та згенерувати новий.

– Не зберігайте пароль доступу до ключа ЕЦП на носії ключової інформації або разом із носієм.

9. Про всі факти втручання в роботу ЕОМ або виявлення порушень вимог цієї Інструкції користувач повинен повідомити про це відповідальному за технічний захист інформації (ТЗІ) в ТОВ «ППЛ 33-35» (Центр обробки даних/ЦОД) на електронну пошту support@ppl33-35.com та на електронну пошту Адміністрації.

10. Користувач несе особисту відповідальність за дотримання правил обробки конфіденційної інформації в автоматизованій системі та виконання цієї Інструкції та інших настанов стосовно роботи в АС.

11. За порушення, що призвели до витоку конфіденційної інформації або її знищення, а також за порушення вимог нормативних документів щодо роботи з конфіденційною інформацією, цієї Інструкції та законодавства винні особи несуть відповідальність згідно з чинним законодавством України.

ЦЕНТР ОБРОБКИ ДАНИХ:
Товариство з обмеженою відповідальністю
«ППЛ 33-35»

Генеральний директор_____ О.О.Федоров

КОРИСТУВАЧ
Место для ввода текста.

Место для ввода текста.