Додаток № 2
до Договору про надання доступу
до Інформаційної
системи портового співтовариства
від «___» _____ 2014 року

Інструкція з антивірусного захисту інформації в автоматизованій системі класу «3» єдиної інформаційної системи портового співтовариства (інформаційної системи портового співтовариства)

Вимоги до системи антивірусного захисту

Комп'ютерним вірусом є паразитуючий програмний код, який обумовлює виконання несанкціонованих команд/програм на ураженому комп'ютері. Вірус розповсюджується у вигляді програм, файлів та макросів. Він впливає на цілісність інформації, програмне забезпечення та (чи) режим роботи обчислювальної техніки, що може привести до відмови комп'ютера, виконання ним дій, що приховані від користувача, і відповідно, до порушення цілісності та доступності інформації або її витоку.

Система антивірусного захисту повинна базуватися на антивірусних продуктах, що мають експертний висновок Державної служби спеціального зв'язку та захисту інформації України для забезпечення можливості контролю проникнення вірусів у максимально короткі строки після їх появи. Перелік антивірусних продуктів, що мають експертний висновок, 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*).

Система захисту файлових служб та служб баз даних повинна забезпечувати захист автоматизованої системи (АС) від комп'ютерних вірусів шляхом перевірки файлів та процесів на цих електронно-обчислювальних машинах (ЕОМ) антивірусним монітором, сканером, що встановлюються на цих ЕОМ.

Найбільш ймовірними вірусними загрозами працездатності автоматизованого робочого місця може бути:

- пошкодження комп'ютерним вірусом файлової структури операційної системи та програмного забезпечення автоматизованої системи;
- знищення даних в енергонезалежній пам'яті комп'ютера (Flash BIOS, CMOS), що може привести до відмови роботи комп'ютера.

Система антивірусного захисту (САЗ) повинна забезпечувати:

- можливість безупинного захисту об'єктів АС відповідно до встановлених вимог та політики безпеки;
- можливість автоматизованого блокування проникнення комп'ютерних вірусів з усіх можливих джерел;
- лікування комп'ютерних вірусів з занесенням інформації про це у відповідні протоколи роботи для забезпечення моніторингу роботи. В разі підозри на зараження невідомими комп'ютерними вірусами та неможливості лікування, САЗ повинна забезпечувати блокування доступу користувачів до цієї інформації;
- можливість оперативного повідомлення відповідальних осіб щодо виникнення критичних чи особливих ситуацій у АС, тобто: виявлення вірусу, збій у системі оновлень, зміна налаштувань САЗ;
- гнучке масштабування при появі нових об'єктів антивірусного захисту у АС;
- ліцензійність та підтримку постачальниками застосованого антивірусного програмного забезпечення.

Обов'язки системного адміністратора АС

Системний адміністратор відповідає за організаційне забезпечення задач керування САЗ та здійснення контролю за її функціонуванням. Системний адміністратор зобов'язаний:

- забезпечувати функціонування САЗ, та контроль виконання її вимог;

- проводити моніторинг роботи антивірусних засобів захисту, та оперативно реагувати на виникнення при цьому критичних ситуацій;

- контролювати своєчасне оновлювання антивірусного програмного забезпечення (оновлення баз проводити не рідше ніж один раз кожні 7 діб);

- оперативно взаємодіяти з користувачами АС та системними адміністраторами організацій у разі виникнення ситуацій, пов'язаних з антивірусним захистом;

- погоджувати свої дії з відповідальним по ТЗІ у разі необхідного внесення змін у роботу програмно-апаратного забезпечення АС, що може бути пов'язано з вірусною загрозою;

- вести облік роботи САЗ.

Обов'язки користувачів АС

Користувачі АС відповідають за дотримання вимог САЗ.

Користувачі АС зобов'язані:

- дотримуватися вимог та рекомендацій щодо захисту інформації у АС від вірусного зараження;

- регулярно оновлювати антивірусні бази (слідкувати за актуальністю антивірусних баз - оновлення проводити не рідше ніж один раз кожні 7 діб);

- в роботі із зовнішніми накопичувачами (магнітні диски, CD-ROM, flash-пам’яті тощо) обов'язково перевіряти їх антивірусною програмою до використання на об'єкті електронно-обчислювальної техніки ЕОТ;

- інформувати системного адміністратора організації про будь-який виявлений вірус, зміни конфігурації або незвичайне поводження комп'ютера або програми та припиняти роботу.

Огляди вірусів

Використовуються різні типи огляду АС:

- огляд вручну або за запитом. Перевіряються обрані файли і папки на ЕОМ;

- огляд у реальному часі. Ця функція безупинно перевіряє на наявність відомих вірусів файли, які читаються/записуються на ЕОМ;

- плановий огляд. Перевіряються обрані файли і папки на АС у запланований час.

Дії системного адміністратора у разі виявлення зараження вірусом

Після одержання інформації про можливість зараження вірусом системний адміністратор:

- інформує системного адміністратора АС та всіх користувачів, що мають доступ до програм або файлів даних, які можуть бути заражені вірусом, про таку ймовірність.

- проводить або ініціює (супроводжує) перевірку ЕОМ АС та зовнішніх накопичувачів користувачів АС засобами САЗ (лікування інфікованого файлу / ізоляція інфікованого файлу / видалення зараженого файлу).

ЦЕНТР ОБРОБКИ ДАНИХ: **Товариство з обмеженою відповідальністю** **«ППЛ 33-35»**	**КОРИСТУВАЧ** Место для ввода текста.
Генеральний директор_____ О.О.Федоров	Место для ввода текста.