

ЕКСПЕРТНИЙ ВИСНОВОК

щодо оцінки комплексу засобів захисту інформації від на базі операційної системи «myLinux» версії 3.1 за критеріями технічного захисту інформації

1 Загальні відомості щодо об'єкта експертизи

Об'єкт експертизи – комплекс засобів захисту інформації на базі операційної системи «myLinux» версії 3.1 (надалі – Комплекс).

Виробник – ТОВ «Майлінукс».

Адреса ТОВ «Майлінукс» – 03113, м. Київ, вул. Шевцова 1, офіс 101.

Експертиза Комплексу виконувалась ДСТСЗІ СБ України на підставі рішення Експертної ради з питань державної експертизи у сфері технічного захисту інформації № 24 від 25.09.03.

2 Загальна характеристика об'єкта експертизи

2.1 Комплекс засобів захисту інформації на базі операційної системи «myLinux» версії 3.1, призначений для забезпечення на програмному рівні захисту інформації, що обробляється на багатокористувальницькому автоматизованому робочому місці, від загроз несанкціонованого доступу до інформації однієї або кількох категорій конфіденційності.

В процесі функціонування Комплекс забезпечує захист інформаційних об'єктів від несанкціонованого доступу за допомогою вбудованих засобів захисту, контроль за виконанням дій користувачів та певних процесів при використанні ними інформаційних об'єктів у відповідності до встановленої політики безпеки, а також можливість самотестування та відновлення після збоїв. Крім того, Комплекс забезпечує стійкість при обмежених відмовах, можливість обмеженої гарячої заміни та ручне відновлення після відмови будь-якого компонента, а також контроль своєї цілісності та самотестування при старті.

2.2 Основними характеристиками Комплексу є:

- забезпечення конфіденційності інформації, що отримується користувачами від інформаційних об'єктів;
- забезпечення цілісності інформаційних об'єктів;
- забезпечення спостережності та керованості комп'ютерної системи.

2.3 Комплекс реалізує сукупність функціональних послуг безпеки, які, згідно НД ТЗІ 2.5-004-99, становлять такий функціональний профіль захищеності інформації:

{КД-2, КА-2, КО-1, КВ-1, ЦД-2, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-2, ДВ-1, НР-2, НИ-3, НК-2, НО-2, НЦ-1, НТ-2}

Позначення та зміст послуг та їх рівнів відповідають НД ТЗІ 2.5-004-99.

3 Нормативні та технічні документи, на відповідність вимогам яких здійснювалась оцінка Комплексу

- Постанова КМ України 29.03.06 №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

- Наказ ДСТСЗІ СБ України № 62 від 29 грудня 1999 року «Про затвердження положення про державну експертизу в сфері технічного захисту інформації».

- НД ТЗІ 2.5-007-2001 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу «1».

- ГОСТ 34.603-99 «Информационная технология. Виды испытаний автоматизированных систем».

- РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов».

- ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».

- ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення». – Введений 01.01.1997.

ЕКСПЕРТНИЙ ВИСНОВОК

щодо оцінки комплексу засобів захисту інформації від на базі операційної системи «myLinux» версії 3.1 за критеріями технічного захисту інформації

- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

- НД ТЗІ 1.1-003-99 «Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

- НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Технічне завдання

4 Методика проведення робіт з експертизи Комплексу за критеріями ТЗІ

Експертні роботи виконувались згідно з розробленими ДСТСЗІ СБ України та узгодженими встановленим порядком документами: «Програма експертних випробувань комплексу засобів захисту інформації на базі операційної системи myLinux» (до вх. ДЦБ №837 від 28.03.06) та «Методика експертних випробувань комплексу засобів захисту інформації на базі операційної системи myLinux» (до вх. ДЦБ №1065 від 27.04.06).

5 Склад програмно-технічних засобів та документів, які надано на експертизу

5.1 Програмні засоби:

Інсталяційний пакет у вигляді інсталяційного CD-диску, контрольна сума якого (алгоритм «md5») складає «aa921e149fdbc431c45b8b9c2ea04086».

5.2 Комплект проектної та експлуатаційної документації:

- Наказ №10-1 від 01.03.04 «Щодо створення комплексу засобів захисту інформації на базі операційної системи myLinux, версії 3.1».

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Технічне завдання (до вх. ДЦБ №138 від 20.01.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Специфікація (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Відомість утримувачів оригіналів (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Пояснювальна записка до технічного проекту (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Тексти програм (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Процеси життєвого циклу програмного засобу (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Програма та методика внутрішніх випробувань (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Протокол внутрішніх випробувань (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Відомість експлуатаційних

ЕКСПЕРТНИЙ ВИСНОВОК

щодо оцінки комплексу засобів захисту інформації від на базі операційної системи «myLinux» версії 3.1 за критеріями технічного захисту інформації

документів (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Формуляр (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Опис застосування (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Опис (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Специфікація пакетів програм, що входять до складу КС (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Опис мови програмування. Команди інтерпретатора bash (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Опис мови програмування. Файли конфігурації політики (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Інструкція адміністратора (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Інструкція користувача (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Організаційні заходи по забезпеченню інформаційної безпеки. Інструкція (до вх. ДЦБ №649 від 10.03.06).

- Комплекс засобів захисту інформації на базі операційної системи myLinux. Дії в аварійних ситуаціях. Інструкція (до вх. ДЦБ №649 від 10.03.06).

- Програма експертних випробувань комплексу засобів захисту інформації на базі операційної системи myLinux (до вх. ДЦБ №837 від 28.03.06).

- Методика експертних випробувань комплексу засобів захисту інформації на базі операційної системи myLinux (до вх. ДЦБ №1065 від 27.04.06).

6 Результати експертних робіт

6.1 Комплектність штатного програмного забезпечення Комплексу відповідає специфікації комплектності.

6.2 Комплекс забезпечує вирішення функціональних завдань згідно експлуатаційної документації.

6.3 За результатами експериментальних випробувань Комплексу встановлено, що:

- рівні реалізованих у Комплексі послуг безпеки відповідають з рівнем гарантій Г-3 вимогам НД ТЗІ 2.5-004-99;

- впроваджені виробником архітектура, середовище, процедура та послідовність розробки, процедури випробування та розповсюдження відповідають специфікаціям рівня гарантій Г-3 критеріїв коректності реалізації функціональних послуг захисту згідно НД ТЗІ 2.5-004-99;

- експлуатаційна документація на Комплекс відповідає специфікаціям рівня гарантій Г-3 критеріїв коректності реалізації функціональних послуг захисту згідно НД ТЗІ 2.5-004-99.

6.5 Результати експертних випробувань щодо кожного пункту «Методики експертних випробувань комплексу засобів захисту інформації на базі операційної системи myLinux» (до вх. ДЦБ №1065 від 27.04.06) викладені у документі «Протокол експертних випробувань комплексу засобів захисту інформації на базі операційної системи myLinux». Матеріали протоколу випробувань свідчать, що зміст реалізованих функціональних послуг безпеки та їх рівні відповідають вимогам Технічного завдання та НД ТЗІ 2.5-004-99.

ЕКСПЕРТНИЙ ВИСНОВОК

щодо оцінки комплексу засобів захисту інформації від на базі операційної системи «myLinux» версії 3.1 за критеріями технічного захисту інформації

7 Висновки

На підставі проведених експертних випробувань за критеріями ТЗІ встановлено, що Комплекс відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у Технічному завданні й паспорті, з рівнем Г-3 оцінки коректності їх реалізації відповідно до НД ТЗІ 2.5-004-99.

Вимоги до умов функціонування Комплексу у випадку використання його для захисту інформації, що становить державну таємницю, наведено у розділі 8 цього Експертного висновку.

8 Вимоги до умов функціонування

Висновки, які наведені в розділі 7 цього документу дійсні тільки за наступних умов:

- в автоматизованій системі, де буде впроваджуватись Комплекс, організаційними та/або технічними заходами повинна бути заблокована можливість завантаження операційних систем цих автоматизованих систем зі змінних носіїв;

- в автоматизованій системі, де буде впроваджуватись Комплекс, організаційними та/або технічними заходами повинен бути забезпечений захист апаратних компонентів автоматизованої системи від несанкціонованого доступу.

Використання Комплексу для захисту інформації, що становить державну таємницю, можливе лише за умов створення комплексної системи захисту інформації (КСЗІ). В цій КСЗІ мають бути впроваджені організаційні та інженерно-технічні заходи щодо дотримання режиму секретності під час обробки інформації, що становить державну таємницю та блокування витоку інформації технічними каналами. Перелік та зміст цих заходів визначається нормативно-правовими актами та нормативними документами України у галузі захисту інформації.

Повнота та якість впроваджених заходів має бути підтверджена результатами Державної експертизи КСЗІ.

9 Термін дії експертного висновку

Термін дії експертного висновку – до 25 липня 2009 р.