



Україна
Знам'янська міська рада Кіровоградської області
Виконавчий комітет

Розпорядження

від 10 липня 2015 р.

№ 87

м. Знам'янка

Про організацію попередніх випробувань
комплексної системи захисту інформації

Відповідно до Закону України “Про захист інформації в автоматизованих системах”, Указів Президента України від 18 вересня 2002 року № 836 “Про заходи щодо забезпечення інформаційної безпеки держави”, від 27 вересня 1999 року №1299 “Про Положення про технічний захист інформації в Україні”, постанови Кабінету Міністрів України від 8 жовтня 1997 року № 1126 “Про затвердження Концепції технічного захисту інформації в Україні“, керуючись п.20 ч.3 ст.42 Закону України “Про місцеве самоврядування в Україні”:

1. Затвердити Методику попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу “1” 4 категорії виконавчого комітету Знам'янської міської ради, що додається.
2. Утворити комісію з проведення попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу “1” 4 категорії виконавчого комітету Знам'янської міської ради згідно з додатком.
3. Комісії з проведення попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу “1” 4 категорії виконавчого комітету Знам'янської міської ради:
 - ▲ провести попередні випробування комплексної системи захисту інформації в автоматизованій системі класу “1” 4 категорії;
 - ▲ скласти та затвердити Протокол попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу “1” 4 категорії;
 - ▲ скласти та затвердити Акт за результатами попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу “1” 4 категорії.
4. Контроль за виконанням даного розпорядження покласти на керуючу справами (секретаря) виконкому Меренкову Л.І.

Міський голова

І.Крижановський

**Методика
попередніх випробувань комплексної системи захисту інформації
в автоматизованій системі класу "1" 4 категорії виконавчого комітету
Знам'янської міської ради**

1. Об'єкт випробувань

1.1 Об'єктом випробувань є комплексна система захисту інформації (далі за текстом – КСЗІ) в автоматизованій системі (далі АС) виконавчого комітету Знам'янської міської ради, яка призначена для обробки інформації з обмеженим доступом (далі за текстом – ІзОД), та відноситься до автоматизованих систем класу “1” 4 категорії.

2. Характеристика та мета випробувань

- 2.1 Вид випробувань: попередні.
- 2.2 Випробування проводиться з метою оцінки відповідності реалізованих заходів захисту вимогам нормативно-правових документів з технічного захисту інформації (далі за текстом – НД ТЗІ) і технічного завдання на КСЗІ (далі за текстом – ТЗ) та встановлення факту готовності КСЗІ та АС в цілому до оброблення ІДТ та проведення державної експертизи.

3. Організація випробувань

3.1. Період та засоби випробувань

3.1.1 Випробування проводиться комісією, призначеною розпорядженням міського голови.

3.1.2 Випробування проводиться згідно з вимогами нормативно-правових документів НД ТЗІ та на підставі даної Методики.

3.1.3 Випробування проводиться в реальних умовах з використанням штатних засобів ОС і КЗЗ та додаткових програмних засобів експлуатації КСЗІ в автоматизованій системі обробки інформації в наступній послідовності:

- ▲ перевірка наявності та повноти комплексу проектної і організаційно - технічної документації на КСЗІ та відповідності її змісту НД ТЗІ;
- ▲ перевірка впроваджених заходів захисту від витоку ІДТ технічними каналами;
- ▲ перевірка впроваджених заходів захисту ІДТ від несанкціонованого доступу;
- ▲ перевірка впровадженої технології отримання, обробки та видачі ІДТ;
- ▲ перевірка підготовленості персоналу.

3.1.4 Випробування проводиться з використанням інформації, що не є ІДТ. Для оцінки проведених перевірок застосовуються методи експертного аналізу та стендові роботи з перевірки працездатності засобів та механізмів захисту.

3.2 Керівні та нормативно-технічні документи

При проведенні випробувань використовувалися такі нормативно-методичні документи:

- ▲ “Порядок організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях”, затверджений постановою Кабінету міністрів України від 02.10.2003 № 1561-12;

- ▲ “Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах”, затверджене постановою Кабінету Міністрів України від 16.02.1998 № 180;
- ▲ НД ТЗІ 1.1-002-99. “Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу”, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;
- ▲ НД ТЗІ 2.5-004-99. “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;
- ▲ НД ТЗІ 2.5-005-99. “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності інформації від несанкціонованого доступу”, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22;
- ▲ НД ТЗІ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі”;
- ▲ НД ТЗІ “Тимчасове положення про категоріювання об’єктів (ТПКО-95)”. Затверджено наказом Державної служби України з питань технічного захисту інформації від 10 липня 1995 №35;
- ▲ СТР-3 ГТК СССР-87 “Специальные требования и рекомендации по защите ЭВТ третьей категории от утечки информации за счет ПЭМИ и наводок” (якщо АС класу “1”, він же об’єкт ЕОТ, другої категорії, то зазначається СТР-2 ГТК СССР-87 “Специальные требования и рекомендации по защите ЭВТ второй категории от утечки информации за счет ПЭМИ и наводок”);
- ▲ НД ТЗІ 2.1-001-2001 “Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення”. Затверджено наказом ДСТЗІ від 09.02.2001 р. № 2. Чинний від 20.02.2001;
- ▲ 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””. Затверджено наказом ДСТСЗІ СБ України від 18.07.2001 № 05. Чинний від 20.07.2001;
- ▲ НД ТЗІ 1.4-001-2000. “Типове положення про службу захисту інформації в автоматизованій системі”, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

4. Результати випробувань

4.1 Перевірка відповідності комплекту документації на КСЗІ вимогам НД ТЗІ

В процесі розробки КСЗІ виготовляється наступний комплект проектних та організаційно-технічних документів:

- ▲ Технічне завдання на створення КСЗІ в АС;
- ▲ План захисту інформації в АС;
- ▲ Розпорядження про організацію КСЗІ в АС класу “1” 4 категорії;
- ▲ Розпорядження про затвердження Положення про СЗІ;
- ▲ Формуляр на АС;
- ▲ Акт категоріювання АС та акт обстеження АС;
- ▲ Модель загроз для інформації в АС (включаючи модель порушника);
- ▲ Положення про службу захисту інформації в АС;
- ▲ Інструкція щодо захисту інформації;
- ▲ Інструкція керівника СЗІ;
- ▲ Інструкція адміністратора безпеки АС;
- ▲ Інструкція користувача АС;
- ▲ Інструкція відповідального за виділене приміщення АС;
- ▲ Інструкція про порядок обліку та використання магнітних носіїв;
- ▲ Інструкція щодо порядку забезпечення антивірусного захисту.

4.2 Перевірка реальних умов експлуатації та заходів захисту інформації від витоку технічними каналами

В процесі проведення випробувань проводиться перевірка обладнання приміщення кімнати №10 міськвиконкому на наявність технічних засобів обмеження доступу в приміщення, охоронної сигналізації, наявність документально оформлених правил обмеження доступу до апаратних ресурсів АС.

Основні та допоміжні технічні засоби обчислювальної техніки АС повинні бути розміщені згідно з планом організації робочого місця по обслуговуванню АС. Проводиться перевірка і оцінка якості монтажних робіт при установці вищезгаданих засобів, кабельного обладнання, мережі електроживлення і заземлення.

4.3 Перевірка заходів захисту інформації від несанкціонованого доступу

В процесі виконання випробувань встановлено, що:

- ▲ на ПЕОМ, яка входить до складу АС повинно бути встановлено КЗЗ, про що в паспорті-формулярі АС повинен бути відповідний запис;
- ▲ спроби завантаження ОС в обхід КЗЗ (шляхом завантаження ОС зі змінних носіїв та/або шляхом переривання процесу завантаження) повинні блокуються програмно-апаратними засобами даного КЗЗ;
- ▲ суб'єкти, що мають доступ до ресурсів АС повинно бути зареєстровані як користувачі та адміністратори КЗЗ;
- ▲ діючі параметри налагодження КЗЗ повинно відповідати параметрам, наведеним у інструкціях та експлуатаційній документації;
- ▲ використання КЗЗ повинно обмежувати використання програмного забезпечення поза вказаним переліком;
- ▲ журнал обліку користувачів повинен вестись відповідно до наведеного в Інструкції щодо захисту ІДТ в АС зразку;
- ▲ дії користувачів щодо доступу до АС та ІДТ повинні реєструватися засобами КЗЗ.

4.4 Перевірка технології отримання, обробки, зберігання та видачі інформації

В процесі виконання випробувань проводиться перевірка порядку обліку, видачі та використання машинних носіїв даних та порядку обліку та реєстрації паперових носіїв. Задіяні організаційні заходи, що перевіряються, повинні відповідати вимогам керівних документів та НД ТЗІ.

В процесі проведення випробувань проводиться перевірка працездатності АС. Користувачі повинні мати можливість виконувати свої службові обов'язки, пов'язані з обробкою ІДТ в АС, згідно з встановленою технологією роботи та з дотриманням встановлених вимог щодо захисту ІДТ.

4.5 Перевірка підготовленості персоналу та інших організаційних заходів

В процесі проведення випробувань проводиться перевірка підготовленості персоналу. Адміністратори та користувачі АС повинні знати положення вказаних вище інструкцій в частині, що їх стосується, свої права, обов'язки та порядок дій.

В процесі проведення випробувань проводиться перевірка організації поточного контролю вимог режиму секретності та інших організаційних заходів.

5. Висновок

5.1 Оцінка повноти і закінчення випробувань

Випробування комплексної системи захисту інформації в АС класу "1" проводиться у повному обсязі у відповідності з затвердженою Методикою. В процесі випробувань повинні бути виконані всі пункту розділу 4. "Методики попередніх випробувань".

5.2 Оцінка результатів випробувань

Комплексна система захисту інформації в АС класу "1" повинна повністю відповідати вимогам технічного завдання та діючих НД ТЗІ.

Комісія
з проведення попередніх випробувань комплексної системи захисту інформації
в автоматизованій системі класу "1" 4 категорії виконавчого комітету
Знам'янської міської ради:

Голова комісії:

Меренкова
Лілія Іванівна - керуюча справами (секретар)
міськвиконкому.

Члени комісії:

Балан Сергій Миколайович - завідувач сектору з питань надзвичайних
ситуацій, охорони праці, екології та
благоустрою міста УМА та ЖКГ;

Головченко
Анатолій Володимирович - старший інспектор з оборонної
і мобілізаційної роботи відділу
інформаційної діяльності та комунікацій
з громадськістю;

Денисов
Олександр Миколайович - начальник відділу ведення Державного
реєстру виборців;

Тесленко
Ірина Володимирівна - головний спеціаліст відділу ведення
Державного реєстру виборців.

Секретар міськвиконкому

Л.Меренкова