УДК 681.3.06
Хлапонін Ю.І.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Запропоновано порівняльний аналіз існуючих засобів захисту (КЗЗ) інформації від несанкціонованого доступу (НСД), які застосовуються при побудові комплексних систем захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах (ІТС).

Ключові слова: технічний захист інформації (ТЗІ), інформаційно-телекомунікаційна система (ІТС), несанкціонований доступ (НСД), комплекс засобів захисту (КЗЗ), комплексна система захисту інформації (КСЗІ).

Вступ. Технічний захист інформації займає особливо важливе місце в загальному комплексі заходів щодо забезпечення національної безпеки України в інформаційній сфері та безпосередньо призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в інформаційно-телекомунікаційних системах (ІТС), циркулює на об'єктах інформаційної діяльності та становить державну та іншу встановлену законом таємницю, віднесена до службової інформації або є відкритою, вимога щодо захисту якої встановлена законом.

Захист інформації в інформаційно-телекомунікаційних системах (далі - ІТС) є складовою частиною робіт по її створенню та експлуатації і повинен здійснюватися на всіх етапах життєвого циклу ІТС.

У відповідності до статті 8 Закону України [1] „інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством".

Комплексна система захисту інформації - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС [2].

КСЗІ складається з організаційних заходів, фізичних засобів захисту, а також:

– комплексу технічного захисту інформації від витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наводів, акустичні, віброакустичні, оптичні та інші канали;

– комплексу засобів захисту (КЗЗ) від несанкціонованого доступу (НСД) до інформаціїї, який може здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо.

Порядок обробки інформації в ІТС регламентується прийнятою в організації політикою безпеки інформації (information security policy) як сукупності законів, правил, обмежень, рекомендацій, інструкцій тощо [2].

Для реалізації частини політики безпеки інформації, що покладається на програмні засоби захисту і відповідає реальній моделі загроз, КСЗІ повинна мати наступні функціональні можливості:

– забезпечення входу користувача до системи та завантаження ОС за умови введення ідентифікатора та пароля;

– блокування входу до системи після визначеної кількості невдалих спроб та після закінчення терміну дії пароля;

– реєстрація дій користувачів по відношенню до ресурсів системи;

– контроль за інсталяцією програмного забезпечення;

– розмежування доступу на рівні логічних дисків, каталогів, файлів ОС;

– розмежування доступу та контроль за запуском програм та програмних комплексів

користувачами;

– розмежування доступу до виконання окремих функцій спеціального програмного забезпечення ІТС установи;

– розмежування доступу до об'єктів баз даних;

– блокування сеансу роботи користувача з наступною його автентифікацією при відсутності активності користувача зверх встановленого періоду часу;

– антивірусний захист;

– контроль цілісності КЗЗ.

Примітка: *Необхідно також визначитися із необхідністю використання наступних засобів захисту інформації:*

- система виявлення уразливостей;
- система виявлення вторгнень;
- система захисту від спаму;
- системи захисту від „шпигунського" (Spyware) програмного коду;
- засобів захисту периметру мереж.

Програмне забезпечення захищається організаційними заходами та КЗЗ від НСД. Відповідно до [2] - комплекс засобів захисту; КЗЗ (trusted computing base; TCB) - сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Аналіз існуючих досліджень. На сьогоднішній день розроблені, мають Експертний висновок та застосовуються такі комплекси засобів захисту інформації від НСД як Лоза-1, Лоза-2, Гриф, Гриф-Мережа, Рубіж-РСО.

Метою даної роботи є проведення порівняльного аналізу існуючих засобів захисту інформації від НСД, які застосовуються при побудові комплексних систем захисту інформації (КСЗІ) в ІТС.

Основна частина дослідження.

Порівняльний аналіз комплексу „Гриф" версії 3 та системи ЛОЗА-1 версії 3

1. Комплекс „Гриф" версії 3 відповідає вимогам НД ТЗІ [3] в обсязі функцій, сукупність яких визначається функціональним профілем захищеності:

КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

Система ЛОЗА-1 версії 3, у відповідності до Експертного висновку № 240 від 17.09.2010, реалізує такий функціональний профіль захищеності:

КД-2, КА-2, КО-0, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

У цьому функціональному профілі:

– реалізований нижчій за потрібний рівень функціональної послуги безпеки „Повторне використання об'єктів", а саме, рівень КО-0 (такий рівень не визначений в [4]), замість рівня КО-1;

– реалізований нижчій за потрібний рівень функціональної послуги безпеки „Адміністративна цілісність", а саме, рівень ЦА-1 замість рівня ЦА-2;

– не реалізована функціональна послуга безпеки „Відкат" рівня ЦО-1;

– не реалізована функціональна послуга безпеки „Використання ресурсів" рівня ДР-1;

– не реалізована функціональна послуга безпеки „Стійкість до відмов" рівня ДС-1.

2. Комплекс „Гриф" версії 3 функціонує під керуванням операційних систем MS Windows XP / Vista / 7 / Server 2008.

Система ЛОЗА-1 версії 3, у відповідності до Експертного висновку № 240 від 17.09.2010 та Паспорту на систему, функціонує під керуванням лише операційних систем MS Windows XP/ Vista /7, тобто не функціонує під керування операційної системи MS Windows Server 2008.

3. Комплекс „Гриф" версії 3 забезпечує ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), паролю та носія даних автентифікації (знімного файлового носія або пристрою Touch Memory).

Система ЛОЗА-1 версії 3, у відповідності до Експертного висновку № 240 від 17.09.2010 та експлуатаційної документації, забезпечує автентифікацію користувачів на підставі імені

(псевдоніма), паролю та носія даних автентифікації лише у вигляді знімного файлового носія, тобто не забезпечує автентифікацію з використанням носія даних автентифікації у вигляді пристрою Touch Memory.

4. Функціональні послуги безпеки в комплексі „Гриф" версії 3 реалізовані з рівнем гарантій Г-4 [4].

В системі ЛОЗА-1 версії 3 у відповідності до Експертного висновку № 240 від 17.09.2010 рівень гарантій Г-3, що не дозволяє її використання на ПЕОМ, де обробляється секретна інформація з грифом обмеження „особливої важливості".

Порівняльний аналіз комплексу „Гриф" версії 3 та комплексу „Рубіж-РСО" версії 2.0.

1. Комплекс „Рубіж-РСО" версії 2.0, у відповідності до Експертного висновку № 201 від 26.11.2009, реалізує такий функціональний профіль захищеності:

КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2.

У цьому функціональному профілі:

– реалізований нижчій за потрібний рівень функціональної послуги безпеки „Адміністративна цілісність", а саме, рівень ЦА-1 замість рівня ЦА-2;
– не реалізована функціональна послуга безпеки „Відкат" рівня ЦО-1;
– не реалізована функціональна послуга безпеки „Використання ресурсів" рівня ДР-1;
– не реалізована функціональна послуга безпеки „Стійкість до відмов" рівня ДС-1;
– не реалізована функціональна послуга безпеки „Гаряча заміна" рівня Д№-1;
– реалізований нижчій за потрібний рівень функціональної послуги безпеки „Цілісність комплексу засобів захисту", а саме, рівень НЦ-1 замість рівня НЦ-2.

2. Комплекс „Гриф" версії 3 відповідає вимогам [5] для технологій оброблення інформації Т1 та Т2, що засвідчено діючим Експертним висновком.

Комплекс „Рубіж-РСО" версії 2.0, у відповідності Експертного висновку № 201 від 26.11.2009, забезпечує лише захист інформаційних ресурсів, які зберігаються на зовнішніх носіях, тобто, відповідно до вимог [5], він може використовуватися лише для технології оброблення інформації Т1.

3. Комплекс „Гриф" версії 3 функціонує під керуванням операційних систем MS Windows XP / Vista / 7 / Server 2008.

Комплекс „Рубіж-РСО" версії 2.0, у відповідності до Експертного висновку № 201 від 26.11.2009, функціонує під керуванням лише операційних систем MS Windows 2000/ XP.

4. Дія Експертного висновку № 239 від 13.08.2010 на комплекс „Гриф" версії 3 поширюється на пакети оновлення комплексу, які постачаються виробником на протязі дії Експертного висновку.

У Експертному висновку № 201 від 26.11.2009 на комплекс „Рубіж-РСО" версії 2.0 відомості про те, що його дія поширюється на пакети оновлення комплексу, які постачаються виробником на протязі дії Експертного висновку, відсутні, а у р.8 Експертного висновку зазначено, що він поширюється лише на версії програмних компонентів комплексу, наведені у Додатку Б до Експертного висновку.

5. Комплекс „Рубіж-РСО" версії 2.0, у відповідності до Експертного висновку № 201 від 26.11.2009 та експлуатаційної документації, забезпечує автентифікацію користувачів на підставі імені (псевдоніма), паролю та носія даних автентифікації лише у вигляді знімного файлового носія, тобто не забезпечує автентифікацію з використанням носія даних автентифікації у вигляді пристрою Touch Memory.

6. Комплекс „Гриф" версії 3 забезпечує розмежування доступу користувачів до захищених каталогів файлової системи та файлів даних довільного типу, що зберігаються у відповідних каталогах.

Комплекс „Рубіж-РСО" версії 2.0, у відповідності Експертного висновку № 201 від 26.11.2009, забезпечує розмежування доступу лише до зовнішніх носіїв, тобто не забезпечує розмежування доступу користувачів до захищених каталогів файлової системи та файлів даних довільного типу, що зберігаються у відповідних каталогах.

7. Функціональні послуги безпеки в комплексі „Гриф" версії 3 реалізовані з рівнем гарантій Г-4.

В комплекс „Рубіж-РСО" версії 2.0, у відповідності Експертного висновку № 201 від 26.11.2009 рівень гарантій Г-3, що не дозволяє його використання на ПЕОМ, де обробляється секретна інформація з грифом обмеження „особливої важливості".

Висновки. Запропонований у даній статті порівняльний аналіз існуючих засобів захисту інформації від НСД, які застосовуються при побудові комплексних систем захисту інформації (КСЗІ) в ІТС, дозволить власнику або адміністратору ІТС обрати той чи інший КЗЗ (відповідно спосіб розмежування доступу та автентифікації) в залежності від прийнятої в організації політики безпеки інформації.

ЛІТЕРАТУРА

1. Закон України від 5.07.1994 року № 80/94-ВР. Про захист інформації в інформаційно-телекомунікаційних системах.

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

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

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

5. НД ТЗІ 2.5-007-2007. Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу „1".

6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков – К.: Видавнича група BHV, 2009. - 608 с.

Надійшла: 04. 02. 2012

Рецензент: д.т.н., доц. Толюпа С.В.