УДК 681.324

В.А. Алєксєєв, В.А. Хоменко, О.А. Авраменко

# Додаткова експертиза з технічного захисту інформації в Україні

Рассмотрен подход к проведению дополнительных экспертиз программного обеспечения по технической защите информации, позволяющий выбирать виды и объемы выполняемых работ на основании анализа изменений в объекте экспертизы и его среде безопасности. Применение подхода показано на примере дополнительной экспертизы операционной системы *Windows XP SP*2.

An approach to the reevaluation of software information security is considered. The reevaluation process set and amount have to be chosen on the basis of the analysis of the software and security environment changes. The approach is demonstrated by the example of a supplemental expertise of the Windows XP SP2 operation system.

Розглянуто підхід до проведення додаткових експертиз програмного забезпечення з технічного захисту інформації, який дозволяє обирати види та обсяги виконуваних робіт на підставі аналізу змін у об'єкті експертизи та його середовищі безпеки. Застосування підходу показано на прикладі додаткової експертизи операційної системи *Windows XP SP*2.

**Вступ.** Сертифікацію програмних продуктів спрямовано на отримання їх споживачами формальних гарантій того, що ці продукти відповідають вимогам певних нормативно-технічних документів. Такі гарантії надаються третьою стороною (незалежними експертами) за результатами експертизи продукту. Проведення експертизи потребує наявності експертів, методології та системи оцінок. Експертне оцінювання полягає у визначенні кількісних або порядкових оцінок програмного продукту [1].

Експертиза з технічного захисту інформації (ТЗІ) є окремим напрямом сертифікації програмних продуктів. Більшість держав має власну систему сертифікації з ТЗІ, яка включає в себе регулюючі, нормативні та методологічні документи, організації, уповноважені проводити експертизу, та органи, які контролюють проведення експертиз і видачу сертифікатів.

Як систему оцінок програмного продукту з ТЗІ зазвичай використовуються ранжировані вимоги, множина яких утворює критерії оцінювання. Існує декілька національних та міжнародних критеріїв оцінювання програмних продуктів з ТЗІ [2]. Ці критерії містять два типи оцінок: функціональність об'єкта експертизи (ОЕ) щодо захисту інформації та гарантій щодо реалізації цієї функціональності.

Програмні продукти, які проходять в Україні державну експертизу з ТЗІ, оцінюються за національними критеріями (НК), викладеними у нормативному документі ТЗІ (НД ТЗІ) «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 2.5–004–99) [3]. Порядок проведення та оформлення результатів держаних експертиз визначається «Положенням про державну експертизу в сфері технічного захисту інформації» [4].

**Постановка задачі**

За умов позитивного результату експертизи її замовник отримує експертний висновок, для якого встановлюється певний термін дії [4, 5]. Необхідність встановлення такого терміну обумовлюється можливими змінами у ОЕ або його середовищі безпеки [5], що відбуваються за час експлуатації ОЕ та призводять до зниження довіри до того, що він і надалі відповідає визначеному рівню захищеності інформації. У положенні [4] зазначено, що експертиза може бути *первинною*, *додатковою* та *контрольною*.

*Первинна* експертиза є основним видом експертизи, в якому виконується оцінювання ОЕ за НК і приймається рішення щодо ОЕ.

*Додаткова* експертиза проводиться для ОЕ, стосовно якого відкрилися нові науково-технічні обставини або у зв'язку із закінченням терміну дії експертного висновку.

*Контрольна* експертиза призначається для перевірки висновку первинної або додаткової

експертизи та виконується експертами, які не залучалися до первинної експертизи.

На теперішній час при проведенні всіх видів експертиз експерти керуються одними й тими ж НД [3, 4]. Але зрозуміло, що додаткова експертиза має певні відмінності від первинної, оскільки експерти мають у розпорядженні результати оцінки попередньої експертизи. У зв'язку з цим додаткову експертизу доцільно проводити особливим чином. У статті запропоновано підхід до проведення додаткових експертиз та наведено практичний приклад його застосування.

**Первинна експертиза**

У проведенні експертизи беруть участь три сторони: замовник – зазвичай розробник, власник або продавець програмного продукту, організатор – організація, яка проводить експертизу, та координатор – державна установа, яка здійснює контроль за експертизою з боку держави та видає експертні висновки [3]. Первинна експертиза передбачає послідовне проведення певних заходів: надання свідоцтв, їх аналіз, розроблення документації проведення експертизи, проведення випробувань ОЕ, складання експертного висновку (рис. 1).

Свідоцтва, необхідні для проведення експертизи, надаються організатору експертизи її замовником (рис. 1, захід 1). Їх склад та обсяг визначаються вимогами НД ТЗІ. До складу свідоцтв, як правило, входять:

- ОЕ – дистрибутиви з програмним забезпеченням та документацією;
- додаткова документація розробника, включаючи тести; настанови адміністратору щодо безпеки, інсталяції, обслуговування, супроводження та налаштування програмного забезпечення; керівництво для звичайного користувача; матеріали офіційних навчальних курсів; книги, журнали та статті в офіційних виданнях, опублікованих за підтримки розробника;
- результати та матеріали попередніх експертиз цього програмного продукту, у тому числі в інших країнах;
- офіційні веб-ресурси розробника програмного продукту.

Для проведення експертних робіт Організатор залучає експертів – фахівців з ТЗІ, які володіють достатньою кваліфікацією та досвідом. Експерти аналізують надані Замовником свідоцтва з метою виявлення характеристик засобів ТЗІ, реалізованих у ОЕ, та оцінювання їх відповідності вимогам НК (рис. 1, захід 2). До складу наданих Замовником свідоцтв мають входити технічні вимоги з ТЗІ, які включають в себе оцінюваний функціональний профіль захисту (ФПЗ), але на практиці часто експерти власноруч формують цей документ, спираючись на виявлені характеристики засобів ТЗІ. Технічні вимоги є основою для подальших випробувань, оскільки визначають характер та обсяг експертних робіт. У експертизах за «Спільними критеріями» [5] подібний документ називається «Завдання з безпеки». Потім експерти розробляють та узгоджують з координатором документацію проведення експертизи, до складу якої входить програма та методики випробувань функціональних послуг безпеки (ФПБ) і гарантій (рис. 1, захід 3). Ця документація складає основу експертних випробувань, зокрема визначає дії експертів при випробуваннях окремих ФПБ і гарантій (рис. 1, захід 4). У процесі випробувань перевіряються результати тестів розробника, надані Замовником, та за браком тестового покриття формуються і виконуються незалежні тести [6]. Результати випробувань оформлюються у вигляді протоколів і становлять основу для скла-


Рис. 1. Заходи первинної експертизи

дання експертного висновку, який узагальнює рішення експертів стосовно відповідності ОЕ вимогам, визначеним у ФПЗ (рис. 1, захід 5).

**Додаткова експертиза**

Задача цієї експертизи полягає у *підтвердженні* результатів оцінки спроможності захисту інформації ОЕ, отриманих під час первинної експертизи, з урахуванням змін у ОЕ та його середовищі безпеки. Тому її проведення може не потребувати реалізації заходів, передбачених первинною експертизою, у повному обсязі.

Національні нормативні та методичні документи з ТЗІ не містять методологічних положень, які враховують специфіку проведення додаткової експертизи. Найбільш розроблені матеріали, що стосуються цього питання, містяться у міжнародному стандарті [5] «Спільні критерії» у вигляді класу гарантій АМА «Підтримка довіри». Цей клас може застосовуватися до ОЕ, який вже оцінений та отримав експертний висновок. Мета класу АМА полягає у визначенні вимог для підтримки встановленого рівня довіри до ОЕ під час його експлуатації без формальної переоцінки нових версій ОЕ. Він не виключає повністю необхідності переоцінки ОЕ, проте забезпечує її економічну виправданість.

Клас АМА «Підтримка довіри» описує цикл підтримки довіри, який складається з наступних фаз (рис. 2):

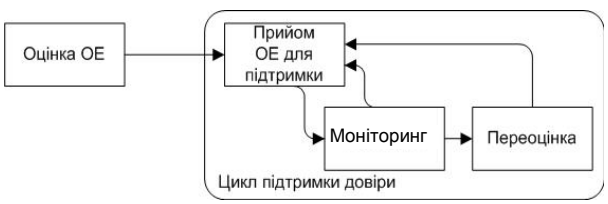


Рис. 2. Цикл підтримки довіри відповідно до стандарту *ISO* 15408–99

- прийом ОЕ для підтримки; розробник встановлює, а незалежний експерт підтверджує плани та процедури з підтримки довіри;
- моніторинг; у контрольних точках циклу підтримки довіри розробник надає експерту свідоцтва того, що довіра до ОЕ підтримується відповідно до встановлених планів та процедур;
- переоцінка; повторна експертиза ОЕ.

Розробники стандарту [5] підкреслюють, що ОЕ не може перебувати у фазі моніторингу постійно, оскільки у певний момент переоцінка стає необхідною. Ступінь змін, які викликають необхідність переоцінки ОЕ, визначаються планом розробника. Крім того, у фазі моніторингу неможливо підвищити рівень довіри до ОЕ.

**Стратегії проведення додаткової експертизи**

Моніторинг не передбачається діючими НД ТЗІ України, тому підтримка гарантій безпеки програмних продуктів забезпечується тільки їх переоцінкою, незалежно від обсягу змін у ОЕ. Отже, цикл підтримки довіри (див. рис. 2) в Україні фактично зводиться до циклу переоцінки, у якому розрізняють оцінену та поточну версію ОЕ (рис. 3).

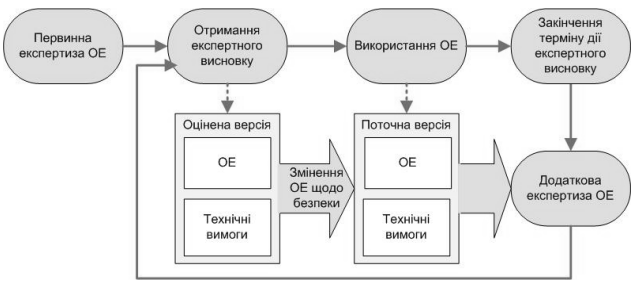


Рис. 3. Цикл переоцінки ОЕ

Для зниження витрат на додаткову експертизу (переоцінку) пропонується проводити її відповідно до стратегії, яка обирається в залежності від рівнів змін у поточній версії ОЕ.

Можна виділити чотири рівня змін щодо безпеки, які вносяться в ОЕ за час його експлуатації до моменту переоцінки:

- нульовий – в ОЕ не відбулося жодних змін (це не виключає змін у його середовищі безпеки);
- реалізаційний – в ОЕ змінилися реалізації окремих функцій безпеки, але функціональність безпеки залишилася незмінною;
- функціональний – у ОЕ відбулися зміни функціональності безпеки (додавання, модифікація або видалення функцій безпеки), які добре локалізовані;
- критичний – обсяг та характер змін у ОЕ значні за обсягом та мають всебічний характер.

Стратегія проведення додаткової експертизи визначається як набір робіт, ранжируваних за рівнями. Кожен наступний рівень включає в себе всі види робіт попередніх. Рівні стратегії відповідають наведеним вище рівням змін у ОЕ (рис. 4) та полягають у наступному:

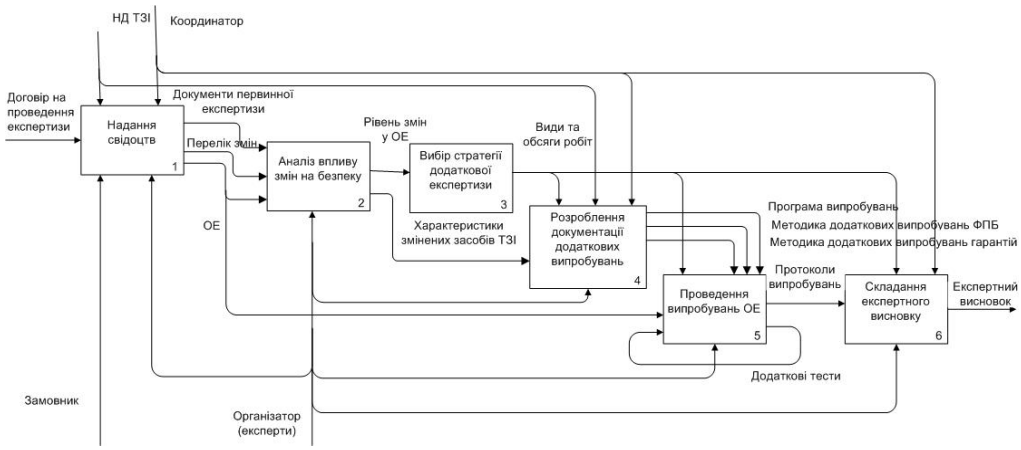


Рис. 5. Заходи додаткової експертизи

• перевірка середовища – перевірка змін у середовищі безпеки ОЕ;

• перевірка реалізації – перевірка коректності змінених реалізацій функцій безпеки;

• перевірка функціональності – переоцінка зміненої функціональності ОЕ щодо забезпечення вимог НД;

• повна переоцінка – проведення повного обсягу робіт, передбаченого первинною експертизою.

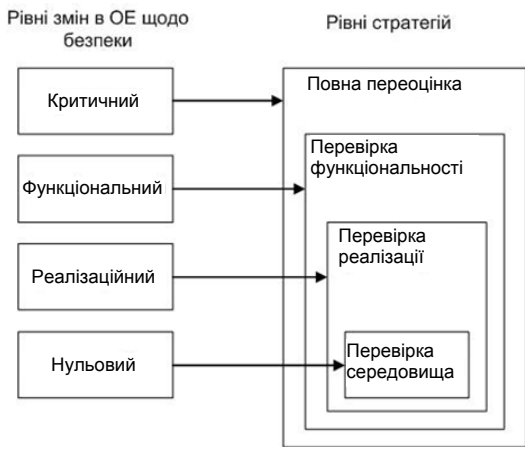


Рис. 4. Рівні змін в ОЕ і стратегій проведення додаткової експертизи

Заходи додаткової експертизи з урахуванням вибору стратегії показано на рис. 5. Для визначення рівня змін у ОЕ реалізується аналіз впливу змін на безпеку (рис. 5, захід 2). На підставі визначеного рівня здійснюється вибір стратегії експертизи (рис. 5, захід 3), яка, в свою чергу, визначає види та обсяги робіт подальших заходів (рис. 5, заходи 4–6).

**Заходи додаткової експертизи**

Розглянемо процеси аналізу впливу змін на безпеку, вибір стратегії додаткової експертизи та розроблення документації (див. рис. 5).

**Аналіз впливу змін на безпеку**

Зміни у ОЕ або його середовищі безпеки можуть обумовлюватися наступними причинами [4, 5] (рис. 6):

• виправленнями помилок, знайдених в оціненому ОЕ;

• змінами функціональних можливостей ОЕ;

• виявленням нових загроз або вразливостей у середовищі безпеки ОЕ;

• змінами у вимогах користувача до захищеності ОЕ.


Рис. 6. Зміни у ОЕ та його середовищі безпеки

Задачами аналізу є класифікація змін у ОЕ, у його середовищі безпеки (див.рис.6) та визначення їх обсягу. Передумовою такого аналізу є надання розробником опису змін ОЕ, його середовища та підтвердження того, що ОЕ продовжує задовольняти свої технічні вимоги з

ТЗІ. Власне технічні вимоги певною мірою можуть бути також змінені. Результатом аналізу є віднесення змін до нульового, реалізаційного, функціонального або критичного рівня.

**Вибір стратегії додаткової експертизи**

Відповідно до запропонованого підходу класифікований рівень змін ОЕ та його середовища безпеки визначає стратегію проведення експертизи (див. рис. 4). Обрана стратегія передбачає певну множину та обсяг робіт. Розглянемо характеристики робіт, які з'являються на кожному рівні стратегії, крім рівня «Повна переоцінка».

***Перевірка середовища.*** На нульовому рівні змін у ОЕ задача експертів полягає у перевірці впливу змін у середовищі безпеки (див. рис.6) на спроможність ОЕ і надалі забезпечувати заявлений рівень захищеності. У змінах до технічних вимог Замовник відображає зміни у вимогах користувачів до безпеки ОЕ та нові загрози і уразливості, виявлені розробником ОЕ на момент проведення експертизи. Характер змін на цьому рівні не повинен вимагати від експертів додаткового аналізу ОЕ. Експертам необхідно тільки оцінити, чи продовжує відповідати моделі безпеки ОЕ (зі зміненими вимогами, новими загрозами і вразливостями) функціональність безпеки, досліджена у попередній експертизі.

***Перевірка реалізації.*** Зміни у реалізації безпеки ОЕ потребують від експерта перевірки того, чи є коректною нова реалізація функції безпеки. Для цього застосовуються випробування, які спираються на методики випробувань ФПБ первинної експертизи, оскільки функціональність та інтерфейси ОЕ залишились незмінними. Експерти можуть прийняти рішення про повне тестування ОЕ або тестування окремих його функцій в залежності від зв'язків змінених компонентів ОЕ з іншими.

***Перевірка функціональності.*** При змінах у функціях безпеки експерту необхідно оцінити їх вплив на відповідність ОЕ функціональному профілю захищеності. Можна виділити три типи змін функцій безпеки – видалення, модифікація та додавання. Для першого типу задача експерта полягає в тому, щоб впевнитись, що видалені функції не брали участі у забезпеченні функціонального профілю захищеності або не мали критичного впливу на нього. Для другого типу змін експерт повинен оцінити, чи не призвела модифікація функції безпеки до порушення профілю. Для третього типу експерт може розглянути, чи забезпечує нова функція заявлений профіль і яким чином.

Слід відзначити, що при кожній переоцінці ОЕ, незалежно від рівня змін у ньому або в його середовищі безпеки, перевірка гарантій безпеки є обов'язковою. Ця перевірка може здійснюватися за методиками первинної експертизи. Підвищення рівня гарантій завжди потребує повної переоцінки ОЕ, оскільки при цьому ускладнюються процедури та методики випробувань як гарантій, так і функціональних послуг безпеки [3]. Зведені види та обсяги робіт, виконуваних за кожної стратегії, надано у таблиці.

**Види робіт у залежності від рівня стратегії**

| Вид роботи | Рівень стратегії | | | |
|---|---|---|---|---|
| | Перевірка | | | Повна переоцінка |
| | середовища | реалізації | функціональності | |
| Перевірка відповідності ФПЗ моделям безпеки ОЕ та його середовища | Часткова | | | Повна |
| Розробка методик випробувань додаткових заходів щодо гарантій безпеки | Для додаткових заходів | | | Для всіх заходів |
| Випробування гарантій | Повне | | | |
| Випробування ФПБ | – | Часткове | | Повне |
| Розробка окремих методик випробувань ФПБ | – | – | Для змінених функцій | Для всіх функцій |
| Інші види робіт, передбачені первинною експертизою | Всі | | | |

**Розроблення документації додаткової експертизи**

На рис. 7 показано документи додаткової експертизи, відображені на основні заходи (див. рис. 5). Множина свідоцтв додаткової експер-

тизи складається з документів первинної експертизи [4, 7] та наступного:

• поточної версії програмного забезпечення ОЕ;

• переліку змін, внесених у ОЕ та його середовище безпеки в період з дати проведення первинної експертизи. Кожна позиція переліку має містити ідентифікацію зміненої функції безпеки, модифікованих компонентів ОЕ та опис впливу внесеної зміни на безпеку ОЕ;

• специфікації змін у технічні вимоги з ТЗІ ОЕ (якщо потрібно).

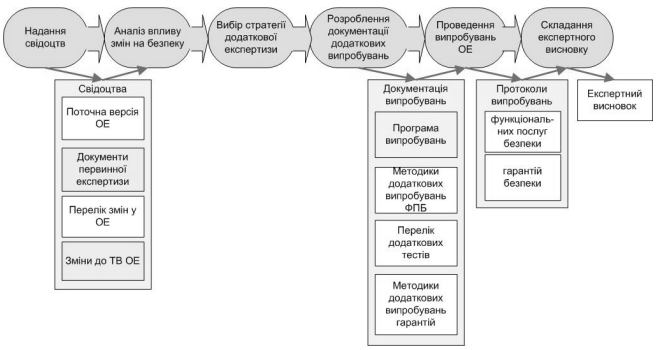


Рис. 7. Документація додаткової експертизи

Програма та методики випробувань ОЕ формуються з урахуванням обраної стратегії додаткової експертизи, виходячи з переліку робіт (див. табл.) та результатів аналізу впливу змін на безпеку.

***Приклад проведення додаткової експертизи***. Запропонований підхід застосовано при проведенні додаткової державної експертизи операційної системи (ОС) *Windows XP SP2*. Ця ОС проходила первинну експертизу з ТЗІ в Україні у 2005 р. [8] та отримала позитивний експертний висновок, термін дії якого закінчився за три роки.

Свідоцтва додаткової експертизи, надані розробником, включали в себе поточну версію ПЗ, документацію та перелік оновлень (у вигляді бюлетенів безпеки), внесених в ОС з часу проведення первинної експертизи.

Аналіз переліку оновлень, проведений експертами, виявив, що поточна версія ОС зазнала змін внаслідок виправлення помилок та усунення виявлених під час експлуатації уразливостей. Для розповсюдження та застосування змін розробник використовує систему оновлення [9], яка забезпечує користувачів ОС відповідними пакетами оновлень, процедурами та програмними засобами. Оновлення класифіковано експертами за класами компонентів ПЗ ОС, на які вони розповсюджуються, а саме: ядро; системні служби та драйвери; застосування та бібліотеки.

Проаналізувавши оновлення безпеки ядра, системних служб та драйверів ОС, експерти дійшли висновку, що ці оновлення не змінюють перелік функціональних можливостей щодо безпеки, визначений для оціненої версії, а тільки усувають «слабкі місця» та недоліки реалізації. Оновлення безпеки щодо застосувань та бібліотек, експертами не аналізувалися, оскільки вони не стосуються власне функціональності безпеки ОЕ. Спираючись на результати аналізу впливу змін на безпеку, рівень змін у поточній версії ОС було визначено як реалізаційний, що відповідає стратегії рівня «Перевірка реалізації».

Перевірка відповідності моделі безпеки ОС існуючому середовищу безпеки призвела до розширення моделі безпеки щодо протидії загрозі несвоєчасного оновлення ОС. До технічних вимог було внесено зміни, які специфікують додаткові заходи гарантій безпеки, пов'язані з оновленням ОС. Для випробувань додаткових заходів експерти розробили відповідну методику.

Проведення випробувань складалося з виконання наступних робіт:

• повного випробування гарантій ОС за методикою первинної експертизи та розробленою методикою додаткової експертизи;

• випробування функціональних послуг безпеки за методикою первинної експертизи у вигляді повторного тестування функцій безпеки ОС.

Проведення експертизи показало, що використання запропонованого підходу дозволило зосередити зусилля експертів на оцінці коректності змін у ОЕ.

**Висновки.** Обсяг робіт, які проводяться при експертизі з ТЗІ, має відповідати умові економічної виправданості. Наявність результатів первинної експертизи під час додаткової дозволяє,

за певних умов, не виконувати весь обсяг робіт експертизи повторно. Аналіз існуючих підходів до проведення додаткових експертиз показує, що для уникнення надлишкових робіт та постійної підтримки гарантій безпеки ОЕ можна застосовувати моніторинг його безпеки під час експлуатації. Але такий підхід не може застосовуватися в Україні, оскільки не відповідає національним НД. Запропонований підхід, заснований на визначенні видів та обсягів робіт експертизи в залежності від змін, які відбулися у ОЕ та його середовищі безпеки, дозволяє обґрунтовано знижувати витрати на проведення додаткової експертизи. Подальша розробка цього підходу потребує деталізації і уточнення класів змін, рівнів стратегій проведення експертизи та дослідження методів оцінки змін щодо ОЕ.


1. *Математика* и кибернетика в экономике: Словарь–справочник. – М.: Экономика, 1975 – 699 с.
2. *Алексєєв В.А.*, *Хоменко В.А.* Використання положень «Спільних критеріїв» при проведенні експертизи з технічного захисту інформації в Україні. // Спеціальні телекомунікаційні системи та захист інформації: Зб. наук. пр. – К.: ДСТСЗІ, 2006. – № 2(11). – С. 43–52.
3. *НД ТЗІ* 2.5–004–99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – 60 с.
4. *Про* затвердження Положення про державну експертизу в сфері технічного захисту інформації. Наказ ДСТСЗІ СБ України від 16 травня 2007 року № 93. – 14 с.
5. *ГОСТ* Р ИСО/МЭК 15408–1. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – 53 с.
6. *Алексєєв В.А.*, *Авраменко О.А.*, *Хоменко В.А.* Організація тестування при проведенні оцінки безпеки програмного забезпечення. // Спеціальні телекомунікаційні системи та захист інформації: Зб. наук. пр. – К.: ДСТСЗІ, 2006. – № 2 (11). – С. 25–42.
7. *НД ТЗІ* 3.7–001–99 Методичні вказівки щодо розроблення технічного завдання на створення системи технічного захисту інформації в автоматизованій системі. – 16 с.
8. *Веб-вузол* «Майкрософт Украина». Розділ «Державна експертиза» – http://www.microsoft.com/Ukraine/ Security/Expert/Default.mspx
9. *Веб-вузол* Windows Update корпорації Microsoft – http://windowsupdate.microsoft.com/


Поступила 10.07.2009
Тел. для справок: (044) 526-6321 (Киев)


●

В.А. Алексеев, В.А. Хоменко, Е.А. Авраменко

## Дополнительная экспертиза технической защиты информации в Украине

**Введение.** Сертификация программных продуктов направлена на получение потребителями формальных гарантий того, что эти продукты соответствуют требованиям определенных нормативно-технических документов. Такие гарантии предоставляются третьей стороной (независимыми экспертами) по результатам экспертизы продукта. Проведение экспертизы требует наличия экспертов, методологии и системы оценок. Экспертное оценивание заключается в установлении количественных или порядковых оценок программного продукта [1].

Экспертиза технической защиты информации (ТЗИ) – отдельное направление сертификации программных продуктов. Большинство государств имеет собственную систему сертификации по ТЗИ, которая включает в себя регулирующие, нормативные и методологические документы, организации, уполномоченные для проведения экспертизы, и органы, контролирующие ее проведение и выдачу сертификатов.

В качестве системы оценок программного продукта по ТЗИ обычно используются ранжированные требования, множество которых формирует критерии оценивания. В настоящее время существует несколько национальных и международных критериев оценки программных продуктов по ТЗИ [2]. Эти критерии содержат два типа оценок: функциональности объекта экспертизы (ОЭ) относительно защиты информации и гарантий реализации этой функциональности.

Программные продукты, проходящие в Украине государственную экспертизу ТЗИ, оцениваются по национальным критериям (НК), изложенным в нормативном документе ТЗИ (НД ТЗИ) «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа» (НД ТЗИ 2.5–004–99) [3]. Порядок проведения и оформления результатов государственных экспертиз определяется «Положением о государственной экспертизе в сфере технической защиты информации» [4].

**Постановка задачи**

При условии положительного результата экспертизы ее Заказчик получает экспертное заключение, для которого устанавливается определенный срок действия [4, 5]. Не-

обходимость установления такого срока обусловлена возможными изменениями в ОЭ или его среде безопасности [5], происходящими за время эксплуатации ОЭ и приводящими к снижению доверия к тому, что он и в дальнейшем соответствует определенному уровню защищенности информации. В положении [4] отмечено, что экспертиза может быть *первичной*, *дополнительной* и *контрольной*.

*Первичная* экспертиза – основной вид экспертизы, в котором выполняется оценка ОЭ по НК и принимается решение относительно ОЭ.

*Дополнительная* экспертиза проводится для ОЭ, относительно которого открылись новые научно-технические обстоятельства, или в связи с окончанием срока действия экспертного заключения.

*Контрольная* экспертиза назначается для проверки заключения первичной или дополнительной экспертизы и выполняется экспертами, которые не привлекались к первичной экспертизе.

Сегодня при проведении всех видов экспертиз эксперты руководствуются одними и теми же НД [3, 4]. Однако очевидно, что дополнительная экспертиза имеет определенные отличия от первичной, поскольку эксперты имеют в распоряжении результаты оценки предыдущей экспертизы. В связи с этим, дополнительную экспертизу целесообразно проводить особым образом. В статье предложены подход к проведению дополнительных экспертиз и пример его применения.

**Первичная экспертиза**

В этом процессе участвуют три стороны: Заказчик – обычно разработчик, владелец или продавец программного продукта; организатор – организация, которая проводит экспертизу; и координатор – государственное учреждение, осуществляющее контроль экспертизы со стороны государства и выдающее экспертные заключения [3]. Первичная экспертиза предусматривает последовательное проведение определенных мероприятий: предоставление свидетельств, анализ свидетельств, разработка документации проведения экспертизы, проведение испытаний ОЭ, составление экспертного заключения (рис. 1).

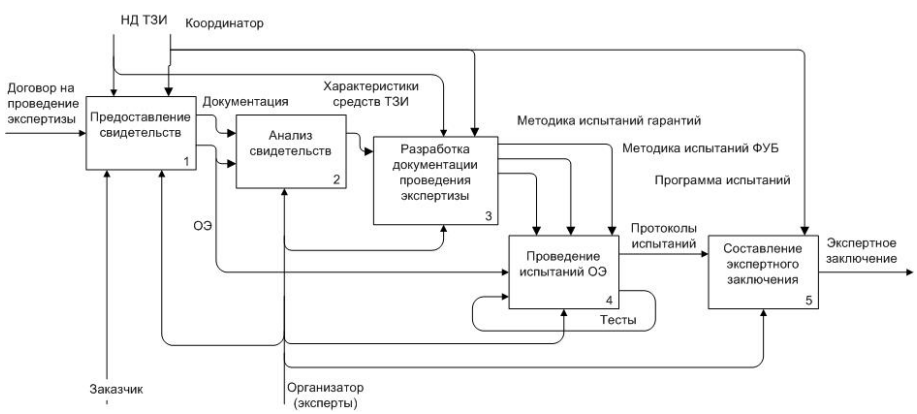


Рис. 1. Мероприятия первичной экспертизы

Свидетельства, необходимые для проведения экспертизы, предоставляются организатору экспертизы ее Заказчиком (рис. 1, мероприятие 1). Их состав и объем определяются требованиями НД ТЗИ. В состав свидетельств, как правило, входят:

- ОЭ – дистрибутивы с программным обеспечением (ПО) и документацией;
- дополнительная документация разработчика, включая тесты; руководства администратора по безопасности, установке, обслуживанию, сопровождению и настройке ПО; руководства для пользователя; материалы официальных учебных курсов; книги, журналы и статьи в официальных изданиях, опубликованные при поддержке разработчика;
- результаты и материалы ранее проведенных экспертиз этого программного продукта, в том числе, в других странах;
- официальные веб-ресурсы разработчика программного продукта.

Для проведения экспертных работ организатор привлекает специалистов по ТЗИ, владеющих достаточной квалификацией и опытом. Эксперты анализируют предоставленные Заказчиком свидетельства с целью выявления характеристик средств ТЗИ, реализованных в ОЭ, и оценки их соответствия требованиям НК (рис. 1, мероприятие 2). В состав предоставляемых Заказчиком свидетельств должны входить технические требования по ТЗИ, включающие в себя оцениваемый функциональный профиль защиты (ФПЗ), но на практике часто эксперты самостоятельно формируют этот документ, опираясь на выявленные характеристики средств ТЗИ. Технические требования являются основой для дальнейшего проведения испытаний, так как определяют характер и объем экспертных работ. В экспертизах, проводимых по «Общим критериям» [5], подобный документ называется «Задание по безопасности». Затем эксперты разрабатывают и согласовывают с координатором документацию проведения экспертизы, в состав которой входит программа и методики испытаний функциональных услуг безопасности (ФУБ) и гарантий (рис. 1, мероприятие 3). Эта документация составляет основу экспертных испытаний, в частности, определяет действия экспертов при испытаниях отдельных ФУБ и гарантий (рис. 1, мероприятие 4). При испытаниях проверяются результаты тестов разработчика, предоставленные Заказчиком, и при недостаточности тестового покрытия формируются и выполняются независимые тесты [6]. Результаты испытаний оформляются в виде протоколов и представляют собой основу для составления экспертного заключения, обобщающего решение экспертов относительно соответствия ОЭ требованиям, определенным в ФПЗ (рис. 1, мероприятие 5).

**Дополнительная экспертиза**

Задача этой экспертизы заключается в *подтверждении* результатов оценки возможности защиты информации ОЭ, полученных при проведении первичной экспертизы, с учетом изменений в ОЭ и его среде безопасности. Поэтому проведение дополнительной экспертизы может не требовать реализации мероприятий, предусмотренных первичной экспертизой, в полном объеме.

Национальные нормативные и методические документы по ТЗИ не содержат методологических положений, учитывающих специфику проведения дополнительной экспертизы. Наиболее разработанные материалы, касающиеся этой проблемы, содержатся в международном стандарте [5] «Общие критерии» в виде класса гарантий АМА «Поддержка доверия». Этот класс может применяться к ОЭ, который уже был оценен и получил экспертное заключение. Цель класса АМА заключается в определении требований для поддержки установленного уровня доверия к ОЭ во время его эксплуатации без формальной переоценки новых версий ОЭ. Он не исключает полностью необходимость переоценки ОЭ, однако, обеспечивает её экономическую целесообразность.

Класс АМА «Поддержка доверия» описывает соответствующий цикл, состоящий из следующих фаз (рис. 2):

- приемка ОЭ для поддержки; разработчик устанавливает, а независимый эксперт подтверждает планы и процедуры по поддержке доверия;
- мониторинг; в контрольных точках цикла поддержки доверия разработчик предоставляет эксперту свидетельства того, что доверие к ОЭ поддерживается в соответствии с установленными планами и процедурами;
- переоценка; повторная экспертиза ОЭ.

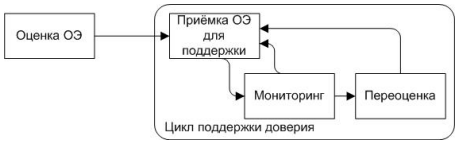


Рис. 2. Цикл поддержки доверия в соответствии со стандартом *ISO* 15408–99

Разработчики стандарта [5] подчеркивают, что ОЭ не может находиться в фазе мониторинга постоянно, поскольку в некоторый момент переоценка становится необходимой. Степень изменений, вызывающих необходимость переоценки ОЭ, определяется планом разработчика. Кроме того, в фазе мониторинга невозможно повысить уровень доверия к ОЭ.

**Стратегии проведения дополнительной экспертизы**

Мониторинг не предусмотрен действующими НД ТЗИ Украины, поэтому поддержка гарантий безопасности программных продуктов обеспечивается только их переоценкой независимо от объема изменений в ОЭ. Таким образом, цикл поддержки доверия (см. рис. 2) в Украине фактически сводится к циклу переоценки, в котором различают оцененную и текущую версии ОЭ (рис. 3).

Для снижения затрат на дополнительную экспертизу (переоценку) предлагается проводить ее в соответствии со стратегией, выбираемой в зависимости от уровня изменений в текущей версии ОЭ. Можно выделить четыре уровня изменений, касающихся безопасности, вносимых в ОЭ за время его эксплуатации до момента переоценки:

- нулевой – не произошло никаких изменений (что не исключает изменений в среде безопасности ОЭ);
- реализационный – изменились реализации отдельных функций безопасности, но функциональность безопасности осталась неизменной;
- функциональный – произошли изменения функциональности безопасности (добавление, модификация или удаление функций безопасности), которые хорошо локализованы;
- критический – объем и характер изменений значительны по объему и имеют всесторонний характер.

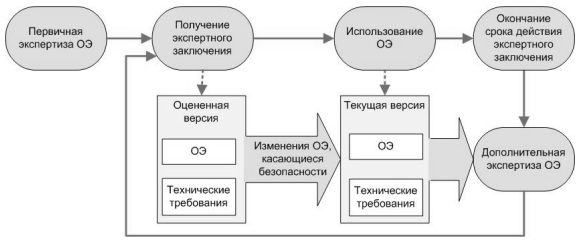


Рис. 3. Цикл переоценки ОЭ

Стратегия проведения дополнительной экспертизы определяется как набор работ, ранжированных по уровням. Каждый следующий уровень включает все виды работ предыдущих. Уровни стратегии соответствуют приведенным выше уровням изменений в ОЭ (рис. 4) и заключаются в следующем:

- проверка среды – проверка изменений в среде безопасности ОЭ;
- проверка реализации – проверка корректности измененных реализаций функций безопасности;
- проверка функциональности – переоценка измененной функциональности ОЭ на предмет обеспечения требований НД;
- полная переоценка – проведение полного объема работ, предусмотренного первичной экспертизой.

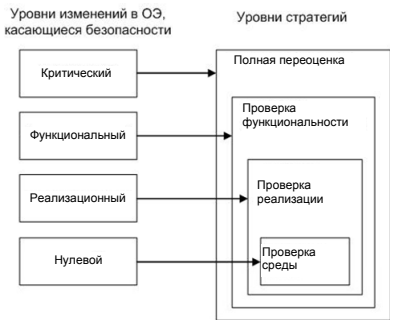


Рис. 4. Уровни изменений в ОЭ и уровни стратегий проведения дополнительной экспертизы

Мероприятия дополнительной экспертизы с учетом выбора стратегии приведены на рис. 5. Для определения уровня изменений в ОЭ реализуется анализ влияния изменений на безопасность (рис. 5, мероприятие 2). На этом уровне осуществляется выбор стратегии экспертизы (рис. 5, мероприятие 3), уровень которой, в свою очередь, определяет виды и объем работ дальнейших мероприятий (рис. 5, мероприятия 4–6).

**Мероприятия дополнительной экспертизы**

Рассмотрим процессы анализа влияния изменений на безопасность, выбора стратегии дополнительной экспертизы и разработки документации (см. рис. 5).

**Анализ влияния изменений на безопасность**

Изменения в ОЭ или его среде безопасности могут быть обусловлены следующими причинами [4, 5] (рис. 6):

- исправлениями ошибок, найденных в оцененном ОЭ;
- изменениями функциональных возможностей ОЭ;
- выявлениями новых угроз или уязвимостей в среде безопасности ОЭ;
- изменениями требований пользователя к защищенности ОЭ.

Задачи анализа – классификация изменений в ОЭ и его среде безопасности (см. рис. 6) и определение объема этих изменений. Предусловием такого анализа является предоставление разработчиком описания изменений ОЭ, его среды и свидетельств того, что ОЭ продолжает удовлетворять своим техническим требованиям по ТЗИ. Собственно технические требования в определенной мере могут быть также изменены. Результатом анализа является отнесение изменений к нулевому, реализационному, функциональному или критическому уровню.

**Выбор стратегии дополнительной экспертизы**

В соответствии с предложенным подходом классифицированный уровень изменений ОЭ и его среды безопасности определяет стратегию проведения экспертизы (см. рис.4). Выбранная стратегия предусматривает определенное множество и объем работ. Рассмотрим характеристики работ, возникающих на каждом уровне стратегии, кроме уровня «Полная переоценка».

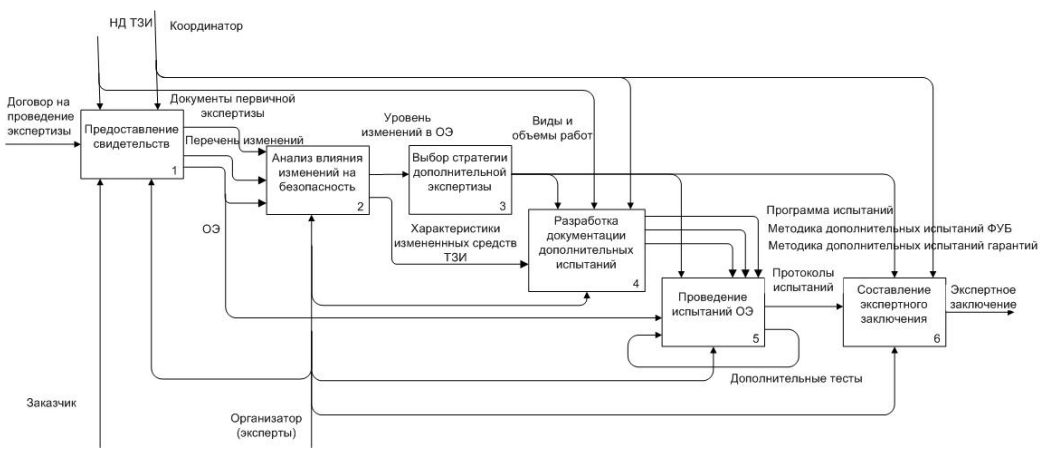


Рис. 5. Мероприятия дополнительной экспертизы

***Проверка среды.*** При нулевом уровне изменений в ОЭ задача экспертов заключается в проверке влияния изменений в среде безопасности (см. рис. 6) на возможность ОЭ и дальше обеспечивать заявленный уровень защищенности. В изменениях к техническим требованиям Заказчик отражает изменения в требованиях пользователей к безопасности ОЭ и новые угрозы и уязвимости, выявленные разработчиком ОЭ на момент проведения экспертизы. Характер изменений на этом уровне не должен требовать от экспертов дополнительного анализа ОЭ. Экспертам необходимо только оценить, продолжает ли соответствовать модели безопасности ОЭ (с измененными требованиям, новыми угрозам и уязвимостями) функциональность безопасности, исследованная в предыдущих экспертизах.


Рис. 6. Изменения в ОЭ и его среде безопасности

***Проверка реализации.*** Изменения в реализации безопасности ОЭ требуют от эксперта проверки того, что новая реализация функции безопасности корректна. Для этого проводят испытания, основанные на методиках испытаний ФУБ первичной экспертизы, поскольку функциональность и интерфейсы ОЭ остались неизменными. Эксперты могут принять решение о полном тестировании ОЭ или тестировании отдельных его функций в зависимости от связей измененных компонентов ОЭ с другими.

***Проверка функциональности.*** При изменениях в функциях безопасности эксперту необходимо оценить их влияние на соответствие ОЭ функциональному профилю защищенности. Можно выделить *три типа* изменений функций безопасности – *удаление*, *модификация* и *добавление*.

Для *первого* типа задача эксперта состоит в том, чтобы убедиться, что удаленные функции не участвовали в обеспечении функционального профиля защищенности или не имели критического влияния на него.

Для *второго* типа изменений эксперт должен

оценить, не привела ли модификация функции безопасности к нарушению профиля.

Для *третьего* – эксперт может рассмотреть, обеспечивает ли новая функция заявленный профиль и каким образом.

Следует отметить, что при каждой переоценке ОЭ, независимо от уровня изменений в нем или в его среде безопасности, проверка гарантий безопасности обязательна. Эта проверка может осуществляться по методикам первичной экспертизы. Повышение уровня гарантий всегда требует полной переоценки ОЭ, так как при этом усложняются процедуры и методики испытаний как гарантий, так и функциональных услуг безопасности [3]. Виды и объемы работ, выполняемых при каждой стратегии, приведены в таблице.

**Виды работ в зависимости от уровня стратегии**

| Вид работы | Уровень стратегии | | | |
|---|---|---|---|---|
| | Проверка | | | Полная переоценка |
| | среды | реализации | функциональности | |
| Проверка соответствия ФПЗ моделям безопасности ОЭ и его среды | Частичная | | | Полная |
| Разработка методик испытаний дополнительных мероприятий, касающихся гарантий безопасности | Для дополнительных мероприятий | | | Для всех мероприятий |
| Испытание гарантий | Полная | | | |
| Испытание ФУБ | – | Частичная | | Полная |
| Разработка отдельных методик испытаний ФУБ | – | – | Для измененных функций | Для всех функций |
| Другие виды работ, предусмотренные первичной экспертизой | Все | | | |

**Разработка документации дополнительной экспертизы**

На рис. 7 показаны документы дополнительной экспертизы, отображенные на основные мероприятия (см. рис. 5). Множество свидетельств дополнительной экспертизы состоят из документов первичной экспертизы [4, 7] и следующего:

- текущей версии ПО ОЭ;
- перечня изменений, внесенных в ОЭ и его среду безопасности за период, начиная с момента проведения первичной экспертизы; каждая позиция перечня должна содержать идентификацию измененной функции безопасности, модифицированных компонентов ОЭ и описания влияния внесенного изменения на безопасность ОЭ;
- спецификации изменений к техническим требованиям по ТЗИ ОЭ (если необходимо).

Программа и методики испытаний ОЭ формируются с учетом выбранной стратегии дополнительной экспертизы, исходя из перечня работ (см. таблицу) и результатов анализа влияний изменений на безопасность.

***Пример проведения дополнительной экспертизы.*** Предложенный подход был применен при проведении дополнительной государственной экспертизы операционной системы (ОС) *Windows XP SP*2. Эта ОС проходила первичную экспертизу ТЗИ в Украине в 2005 г. [8] и получила положительное экспертное заключение, срок действия которого закончился через три года.

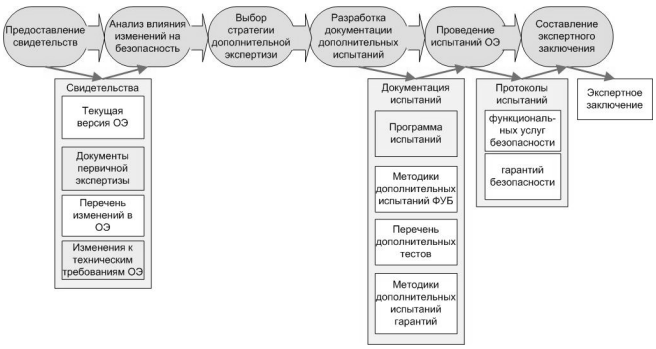


Рис. 7. Документация дополнительной экспертизы

Свидетельства дополнительной экспертизы, предоставленные разработчиком, включали в себя текущую версию ПО, документацию и перечень обновлений (в виде бюллетеней безопасности), внесенных в ОС со времени проведения первичной экспертизы.

Анализ перечня обновлений выявил, что текущая версия ОС претерпела изменения вследствие исправления ошибок и устранения выявленных за время эксплуатации уязвимостей. Для распространения и использования изменений разработчик применяет систему обновлений [9], обеспечивающую пользователей ОС соответствующими пакетами обновлений, процедурами и программными средствами. Обновления были классифицированы экспертами по классам компонентов ПО ОС, на которые они распространяются, а именно: ядро, системные службы и драйверы, приложения и библиотеки.

Проанализировав обновления безопасности ядра, системных служб и драйверов ОС, эксперты пришли к заключению, что эти обновления не меняют перечня относящихся к безопасности функциональных возможностей, установленного для оцененной версии, а только устраняют «слабые места» и недостатки реализации. Обновления безопасности, касающиеся приложений и библиотек, не анализировались, поскольку они не относятся непосредственно к функциональности безопасности ОЭ. Опираясь на результаты анализа влияния изменений на безопасность, уровень изменений в текущей версии ОС был определен как реализационный, что соответствует стратегии уровня «Проверка реализации».

Проверка соответствия модели безопасности ОС существующей среде безопасности привела к расширению модели безопасности в аспекте противодействия угрозе несвоевременного обновления ОС. В технические требования были внесены изменения, специфицирующие дополнительные мероприятия гарантий безопасности, связанные с обновлениями ОС. Для проверки дополни-

тельных мероприятий эксперты разработали соответствующую методику.

Проведение испытаний предусматривало выполнение следующих работ:

- полную проверку гарантий ОС по методике первичной экспертизы и разработанной методике дополнительной экспертизы;
- испытание ФУБ по методике первичной экспертизы в виде повторного тестирования функций безопасности ОС.

Экспертиза показала, что применение предложенного подхода позволило сосредоточить усилия экспертов на оценке корректности изменений в ОЭ.

**Заключение.** Объем работ, проводимых при экспертизе ТЗИ, должен соответствовать условию экономической целесообразности. Наличие результатов первичной экспертизы во время дополнительной позволяет, при определенных условиях, не выполнять весь объем работ экспертизы повторно. Анализ существующих подходов к проведению дополнительных экспертиз показывает, что во избежание выполнения лишних работ и для постоянной поддержки гарантий безопасности ОЭ можно применять мониторинг его безопасности во время эксплуатации. Однако такой подход не приемлем в Украине, поскольку не соответствует национальным НД. Предложенный авторами подход, основанный на определении видов и объемов работ экспертизы в зависимости от изменений, произошедших в ОЭ и его среде безопасности, позволяет обоснованно снижать расходы на проведение дополнительной экспертизы. Дальнейшая разработка этого подхода требует детализации и уточнения классов изменений и уровней стратегий проведения экспертизы, а также исследования методов оценки изменений в ОЭ.

●

*Окончание статьи Л.Ф. Гуляницкого и др.*


7. *Гуляницкий Л.Ф.* Решение задач комбинаторной оптимизации алгоритмами ускоренного вероятностного моделирования // Компьютерная математика: Сб. науч. тр. – К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2004. – № 1. – С. 64–72.
8. *Гуляницкий Л.Ф., Сергиенко И.В.* Метаэвристический метод деформируемого многогранника в комбинаторной оптимизации // Кибернетика и системный анализ. – 2007. – № 6 . – С. 70–79.
9. *Kantardzic M.* Data mining : concepts, models, methods, and algorithms. – Hoboken, NJ: Wiley-Interscience : IEEE Press, 2003. – 345 p. – http://en.wikipedia.org/wiki/Knowledge_ Discovery_in_Databases



Поступила 02.06.2009


Тел. для справок: (044) 526-1589, 526-3603 (Киев)



●