УДК 004.056.53

О.А. Проценко[1], А.В. Блюма[2], А.Д. Кожухівський[1]

[1] *Черкаський державний технологічний університет, Черкаси*
[2] *Департамент фінансів Черкаської облдержадміністрації, Черкаси*

СИСТЕМНИЙ АНАЛІЗ ПРОФІЛЮ ЗАХИЩЕНОСТІ ВІДКРИТИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті порушується проблема організації одного з методів захисту відкритих інформаційних систем, які визначаються доступністю інформації, а також побудова і структура критеріїв їх захищеності.

Ключові слова: *захист інформаційних систем, доступність, ВІС.*

Вступ

Одним із сучасних питань сьогодні є проектування та побудова відкритих інформаційних систем і мереж (надалі – ВІС).

Що ж таке ВІС? Як визначено у Законі України «Про інформацію», до відкритої інформації належить статистична, правова, соціологічна, довідково-енциклопедичного характеру та використовується, для забезпечення діяльності державних органів, або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах, або передається телекомунікаційними мережами [1].

Терміни та визначення.

Обчислювальна система (computer system) – сукупність програмних-апаратних засобів, призначених для обробки інформації.

Автоматизована система (automated system) – організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється.

Комп'ютерна система (computer system, target of evaluation) – сукупність програмно-апаратних засобів, яка подана для оцінки.

Політика безпеки інформації (information security policy) – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкту комп'ютерної системи, або встановлення відповідності між об'єктом і його ідентифікатором, впізнання.

Автентифікація (authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту, встановлення або підтвердження автентичності.

Функціональний профіль (functionality profile) – упорядкований перелік рівнів функціональних послуг, який може використовуватись як формальна специфікація функціональності комп'ютерної системи.

Політика аудиту – події безпеки, які заносяться в журнал реєстрації. Адміністратор отримує можливість слідкувати за діями, які мають відношення до безпеки, наприклад доступом до об'єктів, входом (виходом) з системи.

Результати досліджень

1. Властивості, що відповідають ВІС

В статті ми розглянемо таку властивість інформації, як **доступність** (availability), що відповідає відкритій інформації, системі чи мережі, тобто ВІС (рис. 1).

Рис. 1. Властивості інформації (інформаційних активів)

По-перше. Ми кажемо про **доступність** – це властивість ресурсу (у нашому випадку це веб-сайт), яка полягає в тому, що користувач, який володіє певними повноваженнями, може використовувати ресурс відповідно до правил, не очікуючи довше заданого проміжку часу, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

По-друге. Доступність може забезпечуватись в системі такими послугами, як:

використання ресурсів дозволяє користувачам керувати використанням послуг і ресурсів;

стійкість до відмов гарантує доступність системи (можливість використання інформації, окремих функцій або системи в цілому) після відмови її компонента;

гаряча заміна дозволяє гарантувати доступність системи (можливість використання інформації, окремих функцій або системи в цілому) в процесі заміни окремих компонентів;

відновлення після збоїв забезпечує повернення системи у відомий захищений стан після відмови або переривання обслуговування.

По-третє. Не треба зневажити таким чинником, як **людський фактор**, від якого залежить таж сама доступність.

2. Основні вимоги по захисту ВІС

Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються її **власником (розпорядником)**, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

1. Чітка реалізація послуги ідентифікації та автентифікації – це *політика облікових записів*, яка містить параметри безпеки для паролів і блокування облікових записів.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

2. Ведення аудиту і журналу подій – це *параметри локальної політики,* до якої відносять політику аудита, призначення прав користувачів і параметри безпеки, та *параметри журналу подій*, який використовуються для організації запису системних подій.

3. Наявність систем антивірусного захисту – це *система захисту* від комп'ютерних вірусів, які можуть самостійно копіюватись, розповсюджуватись комп'ютерними мережами, копіювати себе на знімні носії інформації та призводити до порушення роботи комп'ютера, збоїв у функціонуванні комп'ютерних мереж, знищення та/або спотворення інформації, її несанкціонованої передачі каналами зв'язку, порушення конфіденційності, цілісності та доступності інформації.

3. Аналіз захищеності ВІС

3.1. Властивості захищеності. Основними властивостями по захисту ВІС є **доступність** (availability) – властивість ресурсу системи (комп'ютерної системи, послуги, об'єкта комп'ютерної системи, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний [2].

3.2. Функції і механізми захисту. Основними завданнями засобів захисту є ізоляція об'єктів ВІС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання. З одного боку, будь-яка елементарна функція будь-якої з послуг, що реалізуються засобами захисту, може бути віднесена до функцій ізоляції, перевірки або реєстрації. З іншого боку, будь-яка з функцій, що реалізуються засобами захисту, може бути віднесена до функцій забезпечення конфіденційності, цілісності і доступності інформації або керованості ВІС і наочності дій користувачів.

Кожна функція може бути реалізована одним або більше внутрішніми механізмами, що залежать від конкретної ВІС. Водночас одні й ті ж самі механізми можуть використовуватись для реалізації кількох послуг. Наприклад, для розробника слушно реалізувати і адміністративне і довірче керування доступом єдиним набором механізмів.

Реалізація механізмів може бути абсолютно різною. Для реалізації функцій захисту можуть використовуватись програмні або апаратні засоби, криптографічні перетворення, різні методи перевірки повноважень і т. ін. Вибір методів і механізмів практично завжди залишається за розробником. Єдиною вимогою залишається те, щоб функції захисту були реалізовані відповідно до декларованої політики безпеки і вимог гарантій.

Для реалізації певних послуг можуть використовуватись засоби криптографічного захисту. Криптографічні перетворення можуть використовуватись безпосередньо для захисту певної інформації (наприклад, при реалізації послуг конфіденційності) або підтримувати реалізацію послуги (наприклад, при реалізації послуги ідентифікації і автентифікації).

3.3. Забезпечення персональної відповідальності. Кожний співробітник з персоналу ВІС має бути ознайомлений з необхідними положеннями політики безпеки і нести персональну відповідальність за їх додержання. Політика безпеки повинна установлювати обов'язки співробітників, особливо тих, що мають адміністративні повноваження, і види відповідальності за невиконання цих обов'язків. Як правило, це забезпечується в рамках організаційних заходів безпеки.

Однак, коли користувач працює з ВІС, то система розглядає його не як фізичну особу, а як об'єкт, якому притаманні певні атрибути і поводження. Для забезпечення ефективності організаційних заходів необхідна підтримка з боку програмно-апаратних засобів. Комплекс засобів захисту ВІС повинен забезпечувати реєстрацію дій об'єктів-користувачів щодо використання ресурсів системи, а також інших

дій і подій, які так або інакше можуть вплинути на дотримання реалізованої ВІС політики безпеки.

Система повинна надавати користувачам, що мають адміністративні повноваження, можливість проглядати та аналізувати дані реєстрації, що представляються у вигляді журналів реєстрації, виявляти небезпечні з точки зору політики безпеки події, встановлювати їх причини і користувачів, відповідальних за порушення політики безпеки.

3.4. Послуги безпеки.

З точки зору забезпечення безпеки інформації ВІС або комплексу засобів захисту, можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз.

Існує певний перелік послуг, які на підставі практичного досвіду визнані «корисними» для забезпечення безпеки інформації. Вимоги до реалізації даних послуг наведені в НД ТЗІ 2.5-004-99. Вимоги до функціональних послуг розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного з чотирьох основних типів: конфіденційності, цілісності, доступності та наочності.

Згідно з критеріями, кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. Для кожної послуги повинна бути розроблена політика безпеки, яка буде реалізована. Політика безпеки має визначати, до яких об'єктів застосовується послуга. Ця визначена підмножина об'єктів називається захищеними об'єктами відносно даної послуги.

4. Побудова і структура критеріїв захищеності ВІС

В процесі оцінки спроможності ВІС при забезпеченні захисту оброблюваної інформації від несанкціонованого доступу, розглядаються вимоги двох видів:

– вимоги до функцій захисту (послуг безпеки);

– вимоги до гарантій.

В контексті критеріїв ВІС розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного (рис. 2).

З наведеного переліку детальніше розглянемо **критерії доступності**, які відповідають ВІС.

Для того, щоб ВІС могла бути оцінена на відповідність критеріям доступності, комплекс засобів захисту оцінюваної ВІС повинен надавати послуги щодо забезпечення можливості використання ВІС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність ВІС функціонувати у випадку відмови її компонентів.

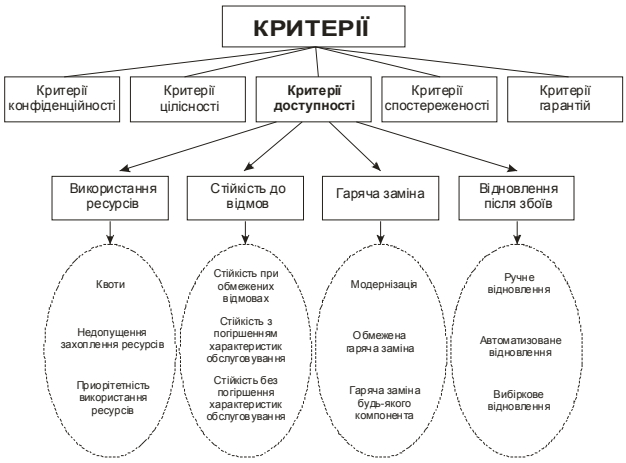

Рис. 2. Структура критеріїв доступності

Доступність може забезпечуватися в ВІС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв [6].

4.1. Використання ресурсів.

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС (табл. 1).

Таблиця 1

Вибірковість керування доступністю послуг КС

Квоти	Недопущення захоплення ресурсів	Пріоритетність використання ресурсів
Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься	Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів КС	Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу і довільним групам користувачів
	Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження	Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача і довільних груп користувачів

4.2. Стійкість до відмов. Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови (табл. 2).

4.3. Гаряча заміна. Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації (табл. 3).

4.4. Відновлення після збоїв.

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення (табл. 4).

Таблиця 2

Функціонування системи після відмови

Стійкість при обмежених відмовах	**Стійкість з погіршенням характеристик обслуговування**	**Стійкість без погіршення характеристик обслуговування**
Розробник повинен провести аналіз відмов компонентів КС		
Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування	Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги	КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента
	Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування	

Таблиця 3

Рівні гарячої заміни

Модернізація	**Обмежена гаряча заміна**	**Гаряча заміна будь-якого компонента**
Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів КС, які можуть бути замінені без переривання обслуговування	Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування
Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	

Висновок

У статті розглянуті питання щодо організації одного з методів захисту відкритих інформаційних систем, які визначаються доступністю інформації, а також побудови і структури критеріїв їх захищеності с позицій системного аналізу.

Таблиця 4

Відновлення після збоїв

Ручне відновлення	**Автоматизоване відновлення**	**Вибіркове відновлення**
Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС		
Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	Після відмови КС або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення КС до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути КС до нормального функціонування	Після будь-якої відмови КС або переривання обслуговування, що не призводить до необхідності заново інсталювати КС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути КС до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування
Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування	Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	

Список літератури

1. Закон України «Про інформацію» від 02.10.92, №2657 – XII.- К., 1992.

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

3. Microsoft. Microsoft Solutions for Security. Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP – Patterns & practices. Microsoft Corporation, 2003.

4. Microsoft. Microsoft Solutions for Security. Windows XP Security Guide v2.0. – Patterns & practices. Microsoft Corporation, 2004.

5. Microsoft. Microsoft Solutions for Security. Руководство по безопасности ОС Windows XP. – Patterns & practices. Microsoft Corporation, 2003.

6. НД ТЗІ. 2.5-008-2002. Вимоги до захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

Надійшла до редколегії 14.05.2015

Рецензент: д-р екон. наук, доц. С.В. Кавун, Харківський інститут банківської справи Університету банківської справи НБУ (Київ), Харків.

СИСТЕМНЫЙ АНАЛИЗ ПРОФИЛЯ ЗАЩИЩЁННОСТИ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

А.А. Проценко, А.В. Блюма, А.Д. Кожуховский

В статье поднимается проблема организации одного из методов защиты открытых информационных систем, которые определяются доступностью информации, а также построение и структура критериев их защищенности.

Ключевые слова: *защита информационных систем, доступность, ОИС.*

SYSTEM ANALYSIS OF PROTECTION PROFILE OF THE OPEN INFORMATION SYSTEMS

A.A. Procenko, A.V. Bluma, A.D. Kozhukhovskiy

The article deals with the problem of the organization of one of protection methods of open information systems, which are defined by information availability, also construction, and criterion structure of their protection.

Keywords: *information systems security, availability, OIS.*