V Функціонування (підтримка і удосконалення СУІБ)

Під час функціонування СУІБ організація повинна:

1. постійно здійснювати удосконалення СУІБ з використанням вимог політики інформаційної безпеки та результатів:
   - перевірок СУІБ;
   - аналізу подій;
   - коректування керівництвом;
2. здійснювати необхідні заходи для усунення причин виникнення невідповідності вимогам СУІБ з метою запобігання їх повторній появі;
3. визначити необхідні попереджувальні дії для усунення можливих невідповідностей вимогам СУІБ та запобіганню їх появі; попереджувальні дії, що застосовуються, мають відповідати можливій проблемі;
4. визначити ризики, що змінилися, та необхідність попереджувальних заходів; пріоритети попереджувальних заходів мають бути визначені на підставі результатів оцінки ризиків;
5. застосовувати досвід, отриманий внаслідок порушення безпеки в інших організаціях та в своїй безпосередньо;
6. повідомляти про дії та удосконалення СУІБ всім зацікавленим сторонам з рівнем деталізації, залежно від обставин;
7. гарантувати, що вдосконалення досягли поставлених цілей.

Отже, використання циклу впровадження СУІБ відповідно до міжнародного стандарту ISO/IEC 27001:2005(E) значно підвищить рівень забезпечення та контролю за інформаційною безпекою в організації, а також дасть змогу керівнику створити конкурентноспроможну, прибуткову, таку, що відповідає законодавству та комерційній репутації організацію.

*Література:**1**. Information technology — Security techniques — Information security management systems — Requirements ISO/IEC 27001:2005(E),* ***2.*** *Information technology — Code of practice for information security management. First edition 2000-12-01 ISO/IEC 17799:2000(E).*

УДК 638.235.231.

АН АЛІЗ ЗАКОНОДАВСТВА В ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ

Василь Цуркан

Спеціальний факультет СБ України ВІТІ НУТУ «КПІ»

Анотація: **На основі аналізу чинного законодавства визначено підхід до забезпечення захисту інформації в автоматизованих системах.**

Summary: **On the Basis of analysis of current legislation, approach was certain to providing of defence of information in the automated systems.**

Ключові слова: **Захист інформації, комплексна система захисту інформації, автоматизована система, несанкціонований доступ, обчислювальна система, захист від несанкціонованого доступу, комплекс засобів захисту, атрибути доступу, довірче та адміністративне керування доступом, критерії оцінки захищеності інформації.**

Відповідно до НД ТЗІ 1. 1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» захисту від різноманітних за своєю сутністю впливів вимагають інформаційні ресурси держави або суспільства в цілому, а також окремих організацій та фізичних осіб, які являють собою цінність, мають відповідне матеріальне вираження. Захистити інформацію – означає створити та підтримувати в дієздатному стані систему заходів, які дозволяють запобігти або ускладнити можливості реалізації різноманітного роду загроз відносно автоматизованої системи, а також знизити потенційні збитки від їх впливу. Система зазначених заходів, що забезпечує захист інформації, називається комплексною системою захисту інформації[1, 2].

Автоматизована система [1] являє собою організаційно-технічну систему, що реалізує інформаційну технологію і об'єднує обчислювальну систему (сукупність програмно-апаратних засобів, призначених для обробки інформації), фізичне середовище, персонал і інформацію, що обробляється. Виділяють три ієрархічні класи автоматизованих систем [3]. Це дозволяє, по-перше, врахувати особливості функціонування кожного з них при розробці профілів захищеності інформації, яка обробляється, а, по-

друге, мінімізувати час на визначення вимог щодо засобів захисту і, таким чином, більш ефективно використати час на розробку комплексної системи захисту інформації.

Розробити комплексну систему захисту означає:

6. сформувати основні загрози інформації, що обробляється в автоматизованій системі, які залежать від характеристик обчислювальної системи, фізичного середовища, персоналу; вони можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. д.) чи відмова елементів обчислювальної системи, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника; останні можуть бути випадковими або навмисними; із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності та доступності інформації;
7. розробити політику безпеки інформації, яка являє собою набір законів, правил, обмежень, рекомендацій, що регламентують порядок обробки інформації та спрямовані на її захист від певних загроз; термін "політика безпеки" може бути застосовано щодо організації автоматизованої, обчислювальної системи, послуги, що реалізується системою; чим дрібніший об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальнішими стають правила;
8. визначити комплекс засобів захисту – сукупність програмно–апаратних засобів, які забезпечують реалізацію політики безпеки інформації; будь-який компонент комп'ютерної системи (сукупність програмно-апаратних засобів, яка подана для оцінки), який внаслідок будь-якого впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина комплексу засобів захисту; для нього ресурси – об'єкти, взаємодією яких він керує відповідно до політики безпеки інформації, що реалізується;
9. урахувати всі можливі способи несанкціонованого доступу до інформації; до основних з них належать:

- безпосереднє звертання до об'єктів з метою одержання певного виду доступу;
- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- модифікація засобів захисту, що дозволяють здійснити несанкціонований доступ до ресурсів;
- впровадження в комп'ютерну систему апаратних механізмів, що порушують її структуру і функції, дозволяють здійснити несанкціонований доступ (діяльність, спрямовану на забезпечення додержання правил розмежування доступу, шляхом створення та підтримки в дієздатному стані системи заходів із захисту інформації);
- описати модель порушника, яку класифікують за рівнем можливостей, що надаються штатними засобами комп'ютерної системи; виділяють чотири рівні цих можливостей; класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:
- перший визначає найнижчий рівень можливостей проведення діалогу з комп'ютерною системою – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій визначається можливістю управління функціонуванням комп'ютерної системи, тобто впливом на базове програмне забезпечення системи, на склад і конфігурацію її устаткування;
- четвертий визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів комп'ютерної системи, аж до включення в її склад власних засобів з новими функціями обробки інформації.

Крім цього необхідно реалізувати основні принципи захисту інформації та керування доступом, а також визначити послуги безпеки [4]. Виділяють наступні принципи:

а) безперервний захист забезпечується протягом всього періоду існування комп'ютерної системи; з моменту створення її об'єкта або його імпорту до системи і аж до знищення або експорту з системи; всі запити на доступ до об'єкта і об'єкта на доступ до інших об'єктів мають контролюватися комплексом засобів захисту;

б) атрибути доступу; кожний об'єкт комп'ютерної системи повинен мати певний набір атрибутів, який включає унікальний ідентифікатор та іншу інформацію, що визначає його права доступу і права доступу до нього; атрибут доступу – термін, що застосовується для опису будь-якої інформації, яка використовується при керуванні доступом і зв'язана з користувачами, процесами або пасивними об'єктами; відповідність атрибутів доступу і об'єкта може бути як явною, так і неявною; атрибути доступу до об'єкта є частиною його подання в комп'ютерну систему;

в) довірче та адміністративне керування доступом; під довірчим керуванням доступом слід розуміти керування, при якому засоби захисту дозволяють звичайним користувачам управляти (довіряють керування) потоками інформації між іншими користувачами та об'єктами свого домену (наприклад, на підставі права володіння об'єктами), тобто призначення і передача повноважень не вимагають адміністративного втручання; адміністративне керуванням доступом – керування, при якому засоби захисту дозволяють управляти потоками інформації між користувачами та об'єктами тільки спеціально авторизованим користувачам;

г) забезпечення персональної відповідальності; кожний співробітник з персоналу автоматизованої системи має бути ознайомлений з необхідними положеннями політики безпеки та нести персональну відповідальність за їх додержання; вона повинна встановлювати 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.

Наявність послуг можна оцінити на основі положень НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». В контексті критеріїв комп'ютерна система розглядається як набір функціональних послуг, які з одного боку являть собою перелік функцій, притаманних комп'ютерній системі, а з іншого – ототожнюються з характеристиками, за наявністю яких можна оцінити можливість протистояння множині загроз безпеці комп'ютерної системи. Виділяють [5] такі критерії:

1. **Функціональні критерії** – оцінюють наявність послуг безпеки; ці критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів:

a) ***загрози конфіденційності*** – несанкціоноване ознайомлення з інформацією під час її переміщення від об'єкта до користувача, запобігання якому забезпечується повнотою реалізації наступних послуг-критеріїв:

- *довірча конфіденційність* дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів;
- *адміністративна конфіденційність* дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів;
- *повторне використання об'єктів* дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо він виділяється новому користувачу або процесу, то не повинен містити інформації, що залишилась від попереднього користувача або процесу;
- *аналіз прихованих каналів* реалізації цієї послуги здійснюється з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами;
- *конфіденційність при обміні* дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище;

b) ***загрози цілісності*** – несанкціонована модифікація інформації; критерії цілісності дозволяють оцінити, наскільки захищена інформація, що обробляється в комп'ютерній системі, від несанкціонованої модифікації; цілісність забезпечується такими послугами:

- *довірча цілісність* дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену;
- *адміністративна цілісність* дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів; основою для ранжування виступає:
- *повернення* забезпечує можливість зупинки виконання операції або послідовності операцій і повернення захищеного об'єкту до попереднього стану;
- *цілісність при обміні* дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище;

c) ***загрози доступності*** – порушення можливості використання комп'ютерних систем або інформації, що в них обробляється; згідно з даним типом загроз критерії дозволяють оцінити можливість використання комп'ютерної системи в цілому, окремих функцій або інформації, що обробляється на певному проміжку часу, і гарантувати її спроможність функціонувати у випадку відмови компонентів; доступність може забезпечуватися такими послугами:

- *використання ресурсів* дозволяє користувачам керувати використанням послуг і ресурсів;
- *стійкість до відмов* гарантує можливість використання інформації, окремих функцій або комп'ютерної системи в цілому після відмови її компонента;

- *гаряча заміна* дозволяє гарантувати можливість використання інформації, окремих функцій або комп'ютерної системи в цілому в процесі заміни окремих компонентів;
- *відновлення після збоїв* забезпечує повернення комп'ютерної системи у відомий захищений стан після відмови або переривання обслуговування;

d) ***загрози несанкціонованих дій*** направлені проти комп'ютерної системи, спроможності комплексу засобів захисту виконувати свої функції, легального доступу до мережі; оцінка відповідальності користувачів за дії чи бездіяльність з їхнього боку здійснюється завдяки критеріям спостережності, а саме наступним послугам:

- *реєстрація* дозволяє контролювати небезпечні для комп'ютерної системи дії;
- *ідентифікація і аутентифікація* дозволяють визначити і перевіряти особистість користувача, що намагається одержати доступ до комп'ютерної системи;
- *достовірний канал* дозволяє гарантувати користувачу можливість безпосередньої взаємодії з комплексом засобів захисту;
- *самотестування* дозволяє комплексу засобів захисту перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій комп'ютерної системи;
- *розподіл обов'язків* дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування; визначає роль адміністратора і звичайного користувача та притаманні їм функції;
- *цілісність комплексу засобів захисту* визначає міру здатності комплексу засобів захисту захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

2. Критерії гарантій оцінюють коректність реалізації послуг безпеки та включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування та експлуатаційної документації; в них вводиться сім рівнів гарантій, які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово зростаючу міру впевненості в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи. Для того, щоб комп'ютерна система одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів:

- *архітектура* повинна забезпечувати гарантії того, що комплекс засобів захисту в змозі повністю реалізувати політику безпеки;
- *середовище розробки* повинно бути таким, щоб гарантувати повну керованість процесів розробки і супроводження комп'ютерної системи, яка оцінюється, з боку розробника;
- *послідовність розробки* - гарантування того, що на кожній стадії розробки (проектування) існує точний опис і реалізація комп'ютерної системи згідно з вихідними вимогами;
- *середовище функціонування* передбачає відсутність в комп'ютерній системі несанкціонованих модифікацій;
- *документація* - опис послуг безпеки, що реалізуються комплексом засобів захисту, настанови адміністратору та користувачу щодо послуг безпеки;
- *випробування* проводяться з метою оцінки спроможності комплексу засобів захисту реалізувати покладені на нього функції щодо захисту комп'ютерної системи від несанкціонованого доступу.

Рекомендації щодо керування безпекою інформації визначені в ДСТУ ISO/IEC TR 13335 – 1,2,3 : 2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій». Перша частина якого описує фундаментальні концепції та моделі даного процесу, друга – аспекти керування та планування, третя – методи захисту.

Організаційне забезпечення завдань керування комплексною системою захисту інформації в автоматизованій системі покладається на службу захисту інформації, порядок функціонуванням якої визначається НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Згідно з ним, задачею її створення є виконання робіт з визначення вимог до захисту інформації та контроль за його станом в автоматизованій системі, проектування, розроблення і модернізації комплексної системи захисту інформації, а також її експлуатація, обслуговування, підтримка працездатності.

У випадку, якщо в автоматизованій системі планується обробка інформації, порядок обробки і захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформація, що становить державну таємницю), то для обробки такої інформації в цій автоматизованій системі необхідно мати дозвіл відповідного уповноваженого державного органу. Підставою для видачі

такого дозволу є висновок експертизи автоматизованої системи, тобто перевірки відповідності реалізованої комплексної системи захисту інформації встановленим нормам

Якщо порядок обробки і захисту інформації не регламентується законодавством, експертиза може виконуватись в необов'язковому порядку за поданням замовника (власника автоматизованої системи або інформації).

В процесі експертизи оцінюється комплексна система захисту інформації автоматизованої системи в цілому. В тому числі виконується оцінка реалізованих в обчислювальній системі засобів захисту, які слід розглядати як підсистему захисту від несанкціонованого доступу в складі комплексної системи захисту інформації.

Отже, залежно від особливостей функціонування автоматизованої системи необхідно визначити відповідний профіль її захищеності та розробити комплексну систему захисту інформації. При цьому слід врахувати основні принципи забезпечення безпеки інформації та керування доступом. Оцінюючи повноту реалізації послуг безпеки необхідно використати критерії оцінки захищеності інформації.

З точки зору методології в проблемі захисту інформації від несанкціонованого доступу слід виділити два напрями:

- забезпечення і оцінка захищеності інформації в автоматизованій системі, що функціонує;
- реалізація та оцінка засобів захисту, що входять до складу компонентів, з яких будується обчислювальна система.

Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, має бути забезпечення безпеки інформації під час її обробки в автоматизованій системі на всіх стадіях її життєвого циклу, на всіх технологічних етапах обробки інформації та в усіх режимах функціонування.

Література: ***1.*** *НД ТЗІ 1. 1-003-99. «Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».* ***2.*** *Закон України «Про захист інформації в автоматизованих системах».* ***3.*** *НД ТЗІ 2. 5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».* ***4.*** *НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».****5.*** *НД ТЗІ 2. 5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».*

УДК 316.776:351.741:34:650.0128

ЗАГАЛЬНА ПАРАДИГМА ЗАХИСТУ ІНФОРМАЦІЇ: ВИЗНАЧЕННЯ ТЕРМІНІВ

Ігор Громико

Харківський національний університет внутрішніх справ

Анотація: **Визначено новий підхід до розв'язання проблем, що існують в теорії та практиці захисту інформації.**

Summary: **Certain a new approach to decision of problems which exist in a theory and practice of protection of the information in Ukraine.**

Ключові слова: **Парадигма, захист інформації, інформаційна безпека, канали витоку інформації.**

Вступ

В рамках державної політики забезпечення безпеки інформаційних ресурсів вкрай потрібна сучасна методологія ефективного забезпечення безпеки інформації [1]. На сьогоднішній день найбільш структурованою є теорія захисту інформації в інформаційних (автоматизованих) системах (ІС). У цій теорії сформульовано низку аксіом і тверджень (теорем), що розкривають методологію створення й функціонування захищених ІС. Узагальнення цієї теорії, що увібрала світовий досвід боротьби з правопорушеннями в інформаційній сфері, і поширення її на загальну інформаційну сферу дозволило автору сформулювати загальну парадигму захисту інформації [2 – 4]:

Дослідження, проведені автором, показали, що зокрема в теорії захисту інформації слід скоректувати ряд положень та визначень термінів.

Невизначеність, неточність приводить до утворення командно-бюрократичної системи захисту інформації. Цей порок уразив більшість країн світу і породив негативні наслідки. В США – це ряд