3. *Кравченко Ю. В.* Применение метода последовательного увеличения ранга k-однородного матроида в задаче синтеза структуры псевдоспутниковой радионавигационной системы /Ю. В. Кравченко// Сучасні інформаційні технології у сфері безпеки та оборони. – 2008. – №2(2). – С. 19–22.
4. *Бусленко Н. П.* Лекции по теории сложных систем / *Бусленко Н. П., Калашников В. В., Коваленко И. Н.* – М. : Сов. радио, 1973. – 440 с.

Поступила 24.02.2011р.

УДК 005.040.20(015.1)

Д.П. Галата, НАУ, м. Київ
Б.Я. Корнієнко, к.т.н., НАУ, м. Київ
Л.П. Галата, НАУ, м. Київ
Н.М. Марутовська, к.т.н., НАУ, м. Київ

ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ

An information security policy addresses many issues such as the following: disclosure, integrity, and availability concerns; who may access what information in what manner; basis on which the access decision is mademaximized sharing versus least privilege; separation of duties; who controls and who owns the information; and authority issues.

Політика безпеки інформації (далі – політика безпеки) - набір вимог, правил, обмежень, рекомендацій і т.п., що регламентують порядок обробки інформації і спрямовані на захист інформації від визначених загроз. Термін “політика безпеки” може бути застосований у відношенні локально обчислювальної мережі (ЛОМ), окремого її компонента, послуги захисту, реалізованою системою і т.п. При цьому врахувати те, що політика безпеки інформації в ЛОМ є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи [1].

Постановка задачі

Метою даної статті є дослідження проблеми політики безпеки інформації в автоматизованій системі (АС).

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості операційної системи, фізичного середовища та інші фактори.

Як складові частини загальної політики безпеки в ЛОМ можуть існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватися: інформації (рівня критичності ресурсів АС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких компонентів ЛОМ політика безпеки стосується, а яких – ні).

Політика безпеки повинна бути розроблена таким чином, що б вона не вимагала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації: правові і морально–етичні норми, організаційні (адміністративні) заходи, фізичні, технічні (апаратні і програмні) заходи і визначати правила і порядок застосування в ЛОМ кожного з цих видів [2].

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- безперервності захисту;
- достатності механізмів і заходів захисту і їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна давати гарантії того, що:

- в АС (у кожній окремій складовій частині, у кожній функціональній задачі і т.п.) забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів щодо захисту інформації є рентабельної;
- у будь–якому середовищі функціонування АС забезпечується оцінювання і перевірка захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів АС), звітність (реєстрація, аудит) для всіх критичних з погляду безпеки ресурсів, до яких здійснюється доступ у процесі функціонування ЛОМ;
- персонал і користувачі забезпечені досить повним комплектом документації, що стосується порядку забезпечення захисту інформації;
- усі критичні з погляду безпеки інформації технології (функції) ЛОМ мають відповідні плани забезпечення безупинної роботи і її відновлення у випадку виникнення непередбачених ситуацій;
- враховано вимоги всіх документів, що регламентують порядок захисту інформації в ЛОМ і забезпечується їхнє строге дотримання.

Політика безпеки розробляється на підготовчому етапі (НД ТЗІ 3.7–001–99) створення КСЗІ. Методологія розробки політики безпеки містить у собі

наступні роботи:

- розробка концепції безпеки інформації в ЛОМ;
- аналіз ризиків;
- визначення вимог до заходів, методів і засобів захисту;
- вибір основних рішень по забезпеченню безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення безупинного функціонування ЛОМ;
- документальне оформлення політики безпеки.

Концепція безпеки інформації в ЛОМ викладає систему поглядів, основних принципів, розкриває основні напрямки забезпечення безпеки інформації [3]. Розробка концепції здійснюється після вибору варіанта концепції створюваної ЛОМ і виконується на підставі аналізу наступних факторів:

- правових і (чи) договірних основ;
- вимог до забезпечення безпеки інформації відповідно до задач і функцій ЛОМ;
- загроз, впливу яких піддаються підлягаючі захисту ресурси ЛОМ.

У результаті аналізу повинні бути сформульовані загальні положення безпеки, що стосуються технології обробки інформації в АС:

- мета і пріоритети, яких необхідно дотримуватися в ЛОМ при забезпеченні безпеки інформації;
- загальні напрямки діяльності, необхідні для досягнення цієї мети;
- аспекти діяльності в області безпеки інформації, що повинні зважуватися на рівні організації в цілому;
- відповідальність посадових осіб і інших суб'єктів взаємин в ЛОМ, їхні права й обов'язки по реалізації задач безпеки інформації.

Захист інформації в ЛОМ АС регламентується:

- законами України, іншими нормативно–правовими актами України;
- державними стандартами й іншими нормативними документами по стандартизації;
- нормативно–правовими актами і нормативними документами системи технічного захисту інформації в Україні;
- нормативними документами, що містять вимоги по захисту інформації в ЛОМ міністерств і інших центральних органів виконавчої влади, дія яких розповсюджується на сферу керування цього органа;
- нормативними, організаційно–розпорядницькими й іншими документами, що діють у межах ЛОМ чи АС організації.

Закони України, інші нормативно–правові акти України, державні стандарти, нормативно–правові акти і нормативні документи системи технічного захисту інформації в Україні формують і впроваджують єдиний у державі порядок забезпечення захисту інформації в ЛОМ АС.

Нормативні документи по захисту інформації міністерств і інших

центральних органів виконавчої влади, а також нормативні документи по стандартизації, що не є державними стандартами, враховують особливості, що існують у галузі.

Нормативні, організаційно–розпорядницькі та інші документи, використовувані в межах окремої організації чи ЛОМ, враховують особливості й умови технології обробки інформації в цій організації чи ЛОМ. Ці документи розробляються керівництвом підприємства, що є власником чи розпорядником ЛОМ.

Такими документами можуть бути*:*

- положення про захист інформації в ЛОМ, положення про службу захисту інформації в ЛОМ, інші документи, що входять у План захисту інформації;
- інструкції про порядок реалізації організаційних, первинних технічних і основних технічних заходів щодо захисту, інструкції про порядок введення в експлуатацію КСЗІ, про порядок її модернізації, про порядок обробки інформації з обмеженим доступом в ЛОМ, про порядок використання криптографічних засобів і ін.;
- правила керування паролями в ЛОМ, правила видачі, вилучення й обміну персональних ідентифікаторів, інших атрибутів розмежування доступу;
- інструкції, що встановлюють повноваження і відповідальність персоналу і користувачів;
- плани виконання робіт чи здійснення окремих заходів щодо захисту інформації в ЛОМ.

Розробці підлягають документи, визначені політикою безпеки інформації. При розробці цих документів дозволяється поєднувати деякі з них у виді окремих розділів в одному документі.

Висновок

Таким чином, сучасна політика безпеки визначає є виключно важливою при побудові та експлуатації захищених АС. В багатьох сучасних програмних засобах захисту інформації уже реалізовані готові політики безпеки. Однак слід зазначити, що це зовсім не означає їх механічного застосування. Зрозуміло, що спочатку в конкретній організації має бути проведений ретельний аналіз процесів обробки інформації, на основі якого потім створюється і застосовується конкретна політика безпеки.

1. *Цирлов В.Л.* Основы информационной безопасности.Краткий курс. - М.: Феникс, 2008. – 253с.
2. *Thomas R.* Peltier Information Security Policies, Procedures, and Standards. - P.: Auerbach Publications, 2001. - 312p.
3. http://security.rit.edu/standards/

Поступила 3.03.2011р.