Стаття присвячена питанням створення комплексної системи захисту інформації, розглянуті основні методи та засоби захисту інформації в комп'ютерних системах та мережах, етапи та проблеми її створення

Ключові слова: система захисту інформації, метод захисту інформації, інформаційна безпека

Статья посвящена вопросам создания комплексной системы защиты информации, рассмотрены основные методы и средства защиты информации в компьютерных системах и сетях, этапы и проблемы ее создания

Ключевые слова: система защиты информации, метод защиты информации, информационная безопасность

The article is devoted questions of creation of the complex system of protection of the information, the basic methods and information security facilities in computer systems and networks, stages and problems of its creation are considered

Keywords: system of protection of the information, a method of protection of the information, information security

УДК 65.012.8

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

З.М. Гадецька
Кандидат технічних наук, доцент
Кафедра загально-технічних дисциплін
Академія пожежної безпеки ім. Героїв Чорнобиля
вул. Оноприєнко, 8, м. Черкаси, Україна, 18034
Контактний тел.: 067-304-17-56
E-mail: josi@ukr.net

І.А. Жирякова
Кандидат технічних наук, доцент
Кафедра математичних та комп'ютерних дисциплін
Черкаська філія Європейського університету
вул. Смілянська, 83, м. Черкаси, Україна, 18008
Контактній тел.: 097-298-89-42
E-mail: irena_zh@ukr.net

1. Вступ

У сучасному суспільстві діє відомий принцип: хто володіє інформацією, той володіє світом. Охочих таким чином панувати світом більш ніж достатньо, а отже, існує стійкий попит на інформацію, отриману незаконним шляхом. В подібній ситуації головний біль власника інформації – це її надійний захист.

Безпека інформації являє собою комплексну проблему, яка охоплює широке коло питань, але першочерговим завданням для її розв'язання є, по-перше, слідування трьом основним постулатам захисту інформації, по-друге, співвіднесення рівня необхідної безпеки і витрат на її підтримку. Отже, при побудові системи захисту інформації (СЗІ) слід дотримуватись наступних правил:

1). СЗІ повинна бути адекватна потенційним загрозам, тому при її розробці необхідно визначити такі загрози, оцінити ймовірність їх виникнення та їх можливі наслідки, а потім вибрати адекватні засоби для їх усунення.

2). СЗІ повинна бути комплексною, тобто використовувати не лише програмно-технічні засоби захисту, а й організаційні та правові.

3). СЗІ повинна бути гнучкою і швидко та без зайвих зусиль адаптуватися до нових умов передбачених організаційними заходами.

2. Постановка проблеми

Комплексні СЗІ створюються для віддзеркалення або значного ускладнення реалізації загроз при несанкціонованому доступі до інформації, яка підлягає захисту, з метою оберігання власників і користувачів інформації від нанесення збитку. Отже, тема дослідження щодо створення комплексної СЗІ, зокрема в Черкаській академії пожежної безпеки ім. Героїв Чорнобиля (надалі ВНЗ), є актуальною.

3. Аналіз останніх досліджень і публікацій

Питання щодо створення СЗІ висвітлені в ряді праць українських та зарубіжних вчених, серед яких В. Мельников, П. Хорев, В. Завгородній, Б. Анін, І. Конєв, В. Галатенко, Е. Таілі, А. Ценк [3, 4, 5, 7, 8] та інші. Але кожна з них в основному обмежується перерахуванням загроз і можливостей конкретних засобів захисту

інформації. Разом з тим, залишаються не вирішеними питання практичної реалізації та впровадження подібних систем у ВНЗ України.

4. Результати

Етапи робіт із створення та впровадження комплексної СЗІ у ВНЗ включають [6]:

- обстеження умов функціонування об'єктів захисту та розробку технічного завдання на створення комплексної СЗІ;
- розробка і реалізація проекту комплексної СЗІ;
- введення комплексної СЗІ в експлуатацію.

Вони є фундаментом для побудови успішного комплексу, який зможе забезпечити необхідний рівень захисту. Розглянемо більш докладно реалізації у ВНЗ найбільш трудомісткого етапу – розробку і реалізацію проекту комплексної СЗІ. Основним завданням на даному етапі є вибір методів та засобів інформаційної безпеки, на які досить істотно впливає прогрес в області розвитку інформаційних технологій та міжнародні і національні стандарти [9-11]. Сучасні підходи, як правило, включають:

1). Морально-етичні заходи захисту.

2). Організаційні заходи захисту, що зводяться до регламентації:

- допуску до використання інформаційних ресурсів;
- процесів проведення технологічних операцій з інформаційними ресурсами;
- процесів експлуатації, обслуговування і модифікації апаратних і програмних ресурсів.

3). Програмно-технічні засоби захисту, що полягають в застосуванні методів:

- ідентифікації і аутентифікації;
- розмежування доступу;
- забезпечення і контролю цілісності;
- антивірусного захисту;
- міжмережевого екранування;
- контролю електронної пошти;
- контролю і реєстрації подій безпеки;
- криптографічного захисту;
- контролю віртуальних приватних мереж (VPN);
- централізованого управління системою інформаційної безпеки.

4). Правові заходи захисту в основі яких лежать Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [1] та Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [2].

Розглянемо найбільш актуальні з них, які на сьогоднішній день запропоновані авторами і впроваджуються у ВНЗ.

Наявність великої кількості інформаційних і обчислювальних ресурсів (баз даних і додатків), що використовуються у ВНЗ і функціонують на різних апаратних і програмних платформах, робить актуальним завдання створення і впровадження системи санкціонованого доступу до єдиного інформаційного простору ВНЗ. Здійснення подібного санкціонованого доступу неможливо без:

- відповідного єдиного механізму;
- єдиної політики безпеки і захисту інформації;
- централізованого і безперервного контролю за використанням ресурсів і управління ними.

На рис. 1 представлена схема санкціонованого доступу до інформаційних ресурсів ВНЗ.

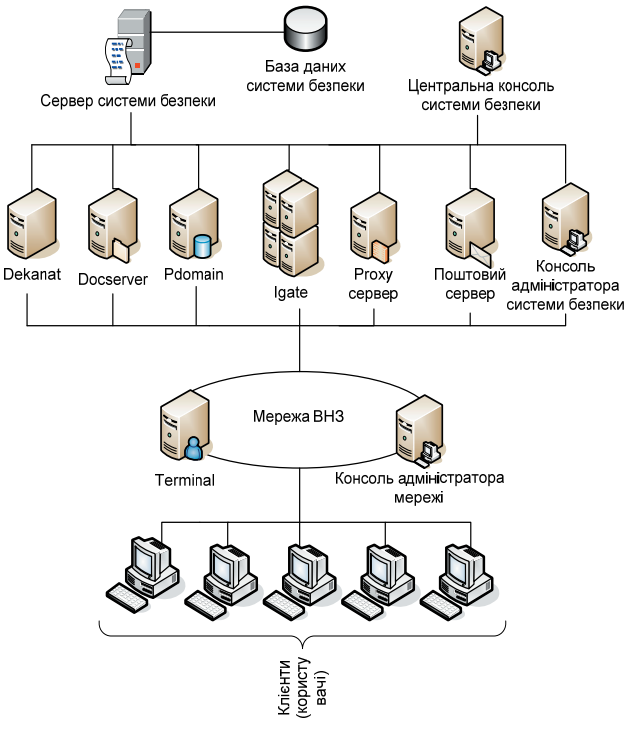

Рис. 1. Схема системи безпеки (санкціонований доступ до ресурсів)

На схемі представлена багатоланкова архітектура, що складається з:

- клієнтського рівня – комп'ютерів користувачів;
- рівня серверів доступу, що реалізовують функції аутентифікації користувачів та управління правами доступу до інформаційних і обчислювальних ресурсів;
- рівня Web-серверів;
- рівня серверів додатків, що забезпечують уніфіковані засоби представлення інформації і функціонування підсистем, що масштабуються; та серверів баз даних.

Надійність засобів управління безпекою в даній схемі також підтримується з допомогою розділенням ролей і обов'язків адміністраторів. Для цього у ВНЗ повинно бути, як мінімум, два адміністратори: адміністратор безпеки і системний адміністратор, а також користувачі.

До засобів технічного захисту інформації, які впроваджуються у ВНЗ, відносяться: контроль входу і виходу співробітників та відвідувачів, охоронна сигналізація, двері із замками, перегородки, телекамери, датчики руху та протипожежної сигналізації, автоматичні засоби пожежегасіння та організація проведення робіт, щодо обладнання серверної аудиторії.

На рис. 2 представлена спроектована схема устаткування серверної кімнати відділу ТЗНП.

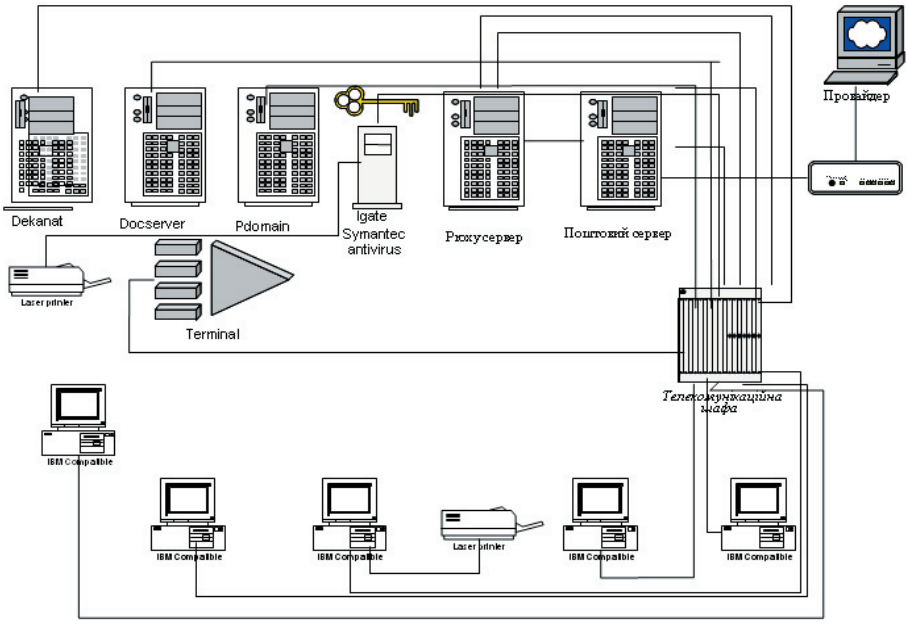

Рис. 2. Схема розміщення устаткування серверної кімнати

Запропонована схема передбачає розміщення серверної кімнати таким чином, щоб проводка повністю охоплювала усі комп'ютери користувачів ВНЗ, забезпечуючи при цьому необхідний рівень захисту від таких небезпек, як збої живлення і несприятливі умови навколишнього середовища.

Але найбільшу увагу, на думку авторів, в СЗІ необхідно звернути на методи програмного захисту, серед яких головну роль займають антивірусні програмні засоби (авторами рекомендується встановлення пакету Norton Antivirus компанії Symantec), впровадження Firewall Outpost Pro на всіх рівнях представлених на рис. 1 та криптографічні засоби захисту (авторами рекомендується встановлення програми Cryptic Disk, кодування та цифровий підпис).

Також як один з організаційних засобів пропонується проводити резервне копіювання даних користувачів раз на тиждень.

5. Висновки

Всі розглянуті в роботі методи та засоби інформаційної безпеки дозволять побудувати комплексну СЗІ в Черкаській академії пожежної безпеки ім. Героїв Чорнобиля. Завдяки впровадженню такої системи захисту стає можливим покращення інформаційного забезпечення ВНЗ та зменшуються втрати інформації. Але треба пам'ятати про те, що ідеальної системи безпеки не існує і всі ці заходи не дають нам 100% впевненості в тому, що інформації нічого не загрожує.

Література

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 81/94-ВР від 05.07.94 (із змінами, внесеними згідно із Законом № 1703-IV (1703-15) від 11.05.2004, в редакції Закону № 2594-IV (2594-15) від 31.05.2005, із змінами, внесеними згідно із Законами № 879-VI (879-17) від 15.01.2009, № 1180-VI (1180-17) від 19.03.2009).
2. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 р. N 373 (відповідно до статті 10 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» № 81/94-ВР від 05.07.94, із змінами, внесеними згідно з Постановою Кабінету Міністрів України № 1700 (1700-2006-п) від 08.12.2006).
3. Галатенко В. А. Стандарты информационной безопасности. – М.: Интернет-Университет Информационных Технологий – ИНТУИТ.РУ, 2004.
4. Грибунин В. Г. Комплексная система защиты информации на предприятии: учеб. пособ. / В. Г. Грибунин, В. В. Чудовский – М.: Академія, 2009. – 416 с.
5. Завгородний В. И. Комплексная защита в компьютерных системах: учеб. пособ. / В. И.Завгородний – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001. – 264 с.
6. Информационная безопасность и защита информации: учеб. пособ. / Степанов Е.А. и др. – М.: Инфра-М, 2002. – 325 с.
7. Мельников В. В. Защита информации в компьютерных системах. / В. В. Мельников – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.
8. Хорев П. Б. Методы и средства защиты информации в компьютерных системах: учеб. пособ. / П. Б. Хорев. – [4-е изд.] – М.: Академия, 2008. – 254 с.
9. ISO/IEC 15408-1. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, 1999.
10. ISO/IEC 15408-2. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements, 1999.
11. ISO/IEC 15408-3. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance require-ments, 1999.