традиційного поняття стійкості функціонування систем і представлена її математична формалізація.

Напрямком подальших досліджень у цій галузі можуть бути методологічні питання реалізації запропонованого підходу, удосконалення математичних моделей і методів забезпечення функціональної стійкості інформаційних керуючих систем і, зокрема, автоматизованої системи управління повітряним рухом.

1. *Малкин И. Г.* Теория устойчивости движения. – М.: Едиториал УРСС, 2010, – 432 с.
2. *Демидович Б. Г.* Лекции по математической теории устойчивости. – М.: Лань, 2008. – 365 с.
3. *Баутин Н. Н.* Методы и приемы качественного исследования динамических систем на плоскости. – М.: Наука, 1990. – 448 с.
4. Большие технические системы: проектирование и управление / *Л. М. Артюшин, Ю. К. Зиатдинов, И. А. Попов, А. В. Харченко. Под ред. И. А. Попова.* – Харьков, Факт, 1997. – 400 с.
5. *Барбашин Е. А.* Введение в теорию устойчивости. – М.: Наука, 2008. – 224 с.
6. *Артюшин Л. М., Машков О. А., Сівов М. С., Дурняк В. М.* Теорія автоматичного керування. – Львів, Політехніка, 2003. – 456 с.
7. *Хинчин А. Я.* Работі по математической теории массового обслуживания. – М.: Либроком, 2010. – 240 с.
8. *Барабаш О. В.* Методология построения функционально устойчивых распределенных информационных систем. – К. НАОУ, 2004. – 214 с.

Поступила 24.03.2011р.

УДК 011.004.06 (013.4)

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

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

The objective of an information system security is to reduce the risk of loss of confidentiality, integrity and availability of information to an acceptable level. The aim of an information system security method is to facilitate the establishment of a comprehensive, cost effective, security programme covering all key information systems. The method should assist users to establish a level of security commensurate with their requirements.

Промислове шпигунство, неправомірне оволодіння та присвоєння інформації, недобросовісна конкуренція – це далеко не весь перелік тих реалій, які супроводжують як державні, так і комерційні структури в їх

розвитку. Тому одним з найактуальніших завдань є створення основних засад формування ефективної системи захисту інформаційних ресурсів.

Аналіз стану захисту інформації в автоматизованих системах України свідчить, що в цілому вирішення цієї проблеми в державі далеке від досконалості.

Постановка задачі

Метою даної статті є дослідження проблеми створення ефективної системи інформаційної безпеки для автоматизованих систем обробки інформації.

Система інформаційної безпеки (СІБ) – це функціонуюча як єдине ціле сукупність засобів, заходів, методів та організацій, яка направлена на ліквідацію зовнішніх та внутрішніх загроз, і має на меті підтримку та розвиток стану захищеності інформаційного середовища суб'єкту безпеки.

Створення СІБ, яка б могла реалізувати всі види захисту, не є вигідним, адже ціна системи перевищує вартість інформації, що захищається. Тому необхідно дотримуватися рівноваги. Це завдання не з легких, тому, коли виникає необхідність забезпечити інформаційну безпеку компанії, керівництво, як правило, звертається до системних інтеграторів. Вони займаються наданням консультаційних послуг, налаштуванням програмного забезпечення та устаткування. В наш час все більше компаній надають такі послуги. Наприклад, АТЗТ АТЛАС – корпорація, один із лідерів серед системних інтеграторів в області телекомунікаційних і інформаційних технологій на ринку України [1].

Компоненти захисту:

1) Системи керування підсистемою захисту (Security management) - система керування забезпечує комплексне керування всіма компонентами захисту, надаючи інтерфейс для керування адміністраторові безпеки та механізми для реалізації політики безпеки.

2) Основні засоби підсистеми захисту:

- засоби розмежування доступу (для локальних мереж: віртуальні мережі (VLAN), для глобальних мереж: міжмережні екрани (Firewall));
- системи виявлення вторгнень (Intrusion Detection System, IDS);
- захист інформації, переданої по каналах зв'язку: криптографія, фізичні засоби захисту, віртуальні приватні мережі (VPN);
- системи ідентифікації, аутентифікації та авторизації:
  - програмні (парольні);
  - апаратно-програмні - з наданням унікального ідентифікатора (смарт-карти, token);
  - біометричні (відбитки пальців, райдужна оборочка ока);
- системи пошуку вразливостей;
- антивірусний захист.

Класифікація міжмережних екранів:

1) за методом виконання:

- апаратно-програмні (спеціалізовані продукти, інтегровані рішення);
- програмні;

2) за місцем розташування:
- для захисту одного комп'ютера;
- класу робочої станції;
- серверного класу;
- прикордонний (мережний);

3) технології:
- фільтри пакетів;
- шлюз сеансового рівня;
- шлюз прикладного рівня;
- брандмауер експертного рівня.

Класифікація засобів VPN:

1) за рівнем еталонної моделі OSI:
- канальний рівень (PPTP, L2F);
- мережний рівень (IPSec);
- транспортний рівень TLS;
- сеансовий SSH/SSL;
- прикладний (захищений обмін повідомленнями - S/MIME);

2) по способу реалізації криптографічних алгоритмів:
- апаратна реалізація
- програмна реалізація

Класифікація систем пошуку вразливостей:

1) виявлення вразливостей шляхом:
- аналіза настроювань (пасивний пошук);
- імітації атак (активний пошук);

2) область сканування:
- мережний сканер;
- системний сканер;
- сканер вразливості додатків (СКБД, WEB- сервер);

3) результат сканування:
- видача списку вразливостей;
- видача рекомендацій (експертні системи);
- усунення вразливостей в автоматичному, напівавтоматичному режимі.

Спеціалісти компанії Парагон мають дещо інший погляд на створення системи інформаційної безпеки [2]. Вони вважають, що для малих і багатьох середніх підприємств весь проект по захисту можна звести до двох пунктів:

- захист персональних комп'ютерів;

- комплекс із інтернет-шлюзу та фаєрвола, що відгороджує мережу підприємства від Всесвітньої мережі та захищає комп'ютери користувачів від проникнення ззовні.

Таблиця 1

Варіанти захисту

Засоби захисту від НСД	Засоби авторизації
	Мандатне керування доступом
	Виборче керування доступом
	Керування доступом на основі ролей
	Ведення журналу
VPN	
Системи моніторингу мереж	Системи виявлення та запобігання вторгнень
	Системи запобігання витоків конфіденційної інформації
Аналізатори протоколів	
Антивірусні засоби	
Міжмережні екрани	
Криптографічні засоби	Шифрування
	Цифровий підпис
Системи резервного копіювання	
Системи безперебійного живлення	Джерела безперебійного живлення
	Резервування навантаження
	Генератори напруги
Системи аутентифікації	Пароль
	Сертифікат
	Біометрія
Засоби запобігання злому корпусів і крадіжок устаткування	
Засоби контролю доступу в приміщення	
Інструментальні засоби аналізу систем захисту: Моніторинговий програмний продукт	
Концепція інформаційної безпеки	
Система керування засобами захисту(політикою безпеки)	
Системи аналізу та моделювання інформаційних потоків	
Організація VLAN	
Служба безпеки	

Захист персональних комп'ютерів

Найголовніше - не використовувати на комп'ютері реальну IP-адресу Інтернету, і тоді зловмисник не зможе підключитися до вашого комп'ютера.

Не можна без попередньої перевірки спеціальними програмами відкривати файли з невідомими розширеннями (або з відомими розширеннями файлів, що виконуються - *.com, .exe, .bat), що були скачані через Інтернет або отримані по електронній пошті [3].

Захист локальних файлів. Встановлювати паролі довжиною не менше 12 букв і ніколи не повідомляйте свій пароль нікому, навіть системному адміністраторові (у нього повинен бути свій пароль). Попросити системного адміністратора обмежити доступ до ваших файлів, крім тих співробітників, кому це необхідно по посадових інструкціях, і максимально обмежити доступ до файлів через мережу. Зберігати найважливіші файли на флеш-карті USB. Обов'язково блокуйте комп'ютер або виключайте його, якщо виходите з офісу (робочого місця). Встановити пароль в BIOS на включення комп'ютера й опломбувати комп'ютер наклейкою з печаткою.

Бути уважним до нових фахівців - це один з основних каналів витоку даних; потрібно записувати їхні паспортні дані й брати розписку про нерозголошення інформації.

Для захисту інформації персонального комп'ютера рекомендують використовувати як мінімум чотири види програм:

1. Антивіруси, такі як Kaspersky Antivirus, DrWeb, Norton Antivirus, Panda, NOD32.

2. Персональний міжмережний екран. Такі програми захищають від проникнення у ваш комп'ютер через мережу й блокують вірусні епідемії. Можна використовувати вбудований в Windows, хоча рекомендуються більш досконалі - Agnitum Outpost, Symantec Personal Firewall і т.д.

3. Утиліти для виявлення програм-шпигунів і троянських програм. Серед безкоштовних рекомендують Ad-aware компанії Lavasoft.

4. Програми резервного копіювання.

Для забезпечення ефективного захисту корпоративних ресурсів від різних зовнішніх і внутрішніх загроз можна застосовувати окремі варіанти захисту наведені в табл.1.

Висновок

Всім відомий вислів «Хто володіє інформацією, той володіє світом» як ніхто інший характеризує значимість інформації, але сьогодні головним завдання є втримати її, щоб вона не втратила свою цінність.

Головною метою створення системи інформаційної безпеки є запобігання або мінімізація можливих фінансових втрат унаслідок порушення конфіденційності, цілісності, доступності інформації.

При побудові нової системи, потрібно намагатися, щоб до її складу ввійшло як найбільше засобів захисту, з урахуванням цінності інформації та коштів, що необхідні на реалізацію цієї системи.

1. http://www.atlas.ua
2. http://www.itc.ua
3. *Барышев М.В., Гуськов А.А.* Методики разработки защищенной системы автоматизации управления промышленным предприятием//Научно-технический вестник - Вип.40 – СП.: 2007.-С. 242-246.

Поступила 31.03.2011р.