УДК 004.056; 004.77-78

М. А. СТРЕЛЬБІЦЬКИЙ, *кандидат технічних наук, доцент, начальник кафедри зв'язку, автоматизації та захисту інформації Національної академії Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький)*

ДЕКОМПОЗИЦІЯ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ СИСТЕМАХ

У статті визначені складові комплексної системи захисту інформації в корпоративних системах на стадії їх модернізації. Наведено їх три організаційні частини: механізми забезпечення захисту інформації; механізми управління механізмами захисту інформації та механізми загальної організації роботи системи. Результатом дослідження є представлена схема системи управління захистом інформації.

Ключові слова: *захист інформації, корпоративні системи.*

Постановка проблеми у загальному вигляді. Широкомасштабне впровадження автоматизованих систем, побудованих з використанням сучасних інформаційних технологій, у структуру управління на всіх рівнях Державної прикордонної служби України (ДПСУ) є об'єктивною реальністю [1]. До певного моменту автоматизація всіх сфер діяльності суспільства і держави здійснювалась без належної уваги до проблем захисту інформації, що призвело до збільшення можливостей несанкціонованого доступу як до державних, так і до приватних інформаційних ресурсів. Прикладом неналежної уваги до питань захисту інформації може служити факт розкрадання інформаційних ресурсів Міністерства оборони і державного департаменту США, що містили більше 400 тисяч секретних

документів, і передача їх власникам скандально відомого Інтернет-порталу Wikileaks.

Останні 20 років існує стійка тенденція до неухильного збільшення числа інформаційних атак на інформаційні ресурси (рис. 1).

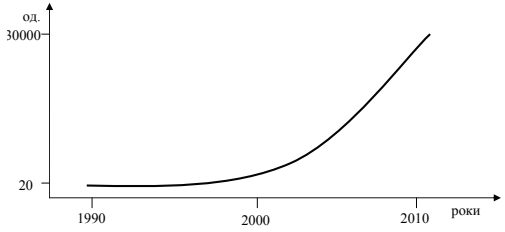

Рис. 1. Кількість офіційно зареєстрованих атак на інформаційні ресурси (за даними http://book.itep.ru)

Показовим є дослідження захищеності web-сайтів, проведене компанією Positive Technologies, результати якого показали, що 81 % з них не відповідають вимогам стандартів з безпеки.

Структура та склад інформаційно-телекомунікаційних систем ДПСУ передбачає збір, обробку та передавання інформації про особу, транспортні засоби та вантажі, які перетинають державний кордон. У цьому аспекті ці підсистеми можуть стати ціллю для зловмисників. Масштаби цієї загрози щорічно зростають. Так, у 2011 році, за офіційними даними, було вилучено тільки з однієї інформаційної системи "Stratfor" інформацію про 68 063 номерів кредитних карток, 859 311 адресів електронної пошти, 50 569 телефонних номерів, 860 160 хешів паролів, з яких біля 11,8 % зловмисники можуть легко отримати самі паролі [2].

З точки зору захисту інформації, повноцінне функціонування сучасних автоматизованих систем можливе тільки за умови забезпечення конфіденційності та цілісності (несуперечливості) інформації, яка циркулює в системі на заданому рівні відповідних показників. Ефективне функціонування інтегрованої інформаційно-телекомунікаційної системи ДПСУ при існуючих загрозах на даний час стає неможливим без забезпечення інформаційної безпеки. Особливе місце в цій проблемі займає технологія управління як організаційна складова процесу захисту інформації.

Метою статті є встановлення складових технології захисту інформації в корпоративних системах (КС) на стадії їх модернізації.

Виклад основного матеріалу дослідження. Найважливішою концептуальною вимогою до інформаційно-телекомунікаційних систем (ІТС) є вимога адаптованості, тобто здатності до цілеспрямованого пристосування при зміні структури, технологічних схем або умов їх функціонування. Для такого функціонування система захисту інформації (СЗІ) має базуватися на чіткій організації та регулярному управлінні.

Під управлінням в ІТС розуміється визначення на кожному кроці її функціонування таких керуючих впливів на елементи системи, наслідком яких буде вирішення одного або декількох функціональних завдань.

Під функціональним завданням розуміється сукупність однорідних у функціональному відношенні операцій, що реалізуються ІТС. З метою здійснення функцій з обробки даних засобами ІТС у рамках кібернетики сформульовані загальні закони управління [3]:

1) будь-яке управління є цілеспрямований процес;

2) будь-яке управління є інформаційний процес, що полягає в зберіганні, опрацюванні та передаванні інформації;

3) будь-яке управління здійснюється в замкнутому контурі, утвореному керуючим і керованим об'єктами, об'єднаними в єдину систему прямою і зворотною лінями зв'язку. На рис. 2 наведено загальну схему організаційно-технологічного управління.

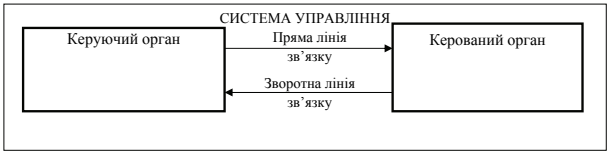

Рис. 2. Загальна схема організаційно-технологічного управління в автоматизованій системі

Рівень розвитку сучасних засобів обчислювальної техніки дозволяє включати до складу СЗІ підсистему підтримки прийняття рішення, яка використовується в центрі управління безпекою КС для автоматизації та підвищення оперативності управління безпекою даних [4].

У результаті декомпозиції СЗІ можна виділити три організаційні частини:

механізми забезпечення захисту інформації;

механізми управління механізмами захисту інформації;

механізми загальної організації роботи системи.

Складовими компонентами системи управління захистом інформації повинні бути механізми, що створюються безпосередньо в КС, а також підрозділи, що створюються для організації та забезпечення їх функціонування.

Сутність механізмів захисту інформації полягає в спостереженні за функціонуванням системи; установлення порогових значень для включення сигналу про події безпеки; сповіщення суб'єктів про ці події; відпрацювання рекомендацій з управління діями СЗІ і застосуванні певних засобів захисту для надання нейтралізуючого впливу на дестабілізуючий фактор (ДФ) та усунення порушення [5, 6].

Для раціонального управління необхідна така технологія, за якої безперервно та регулярно здійснювався б контроль за функціонуванням компонентів КС. На рис. 3 структурно подано схему функціонування системи управління захистом інформації на прикладі інтегрованої ІТС "Гарт".

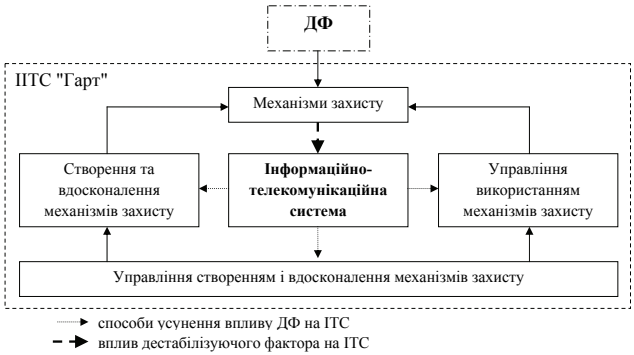

Рис. 3. Схема функціонування системи управління захистом інформації

При створенні й організації функціонування системи управління розглядаються два види процесів:

1) створення механізмів захисту інформації, необхідних і достатніх для надійного захисту інформації для самого загального випадку потенційно можливих ДФ;

2) організація ефективного управління використанням і вдосконаленням (для раніше неврахованих випадків ДФ) механізмів захисту інформації.

У механізмах забезпечення захисту можна виділити два організаційних компоненти: постійні (вбудовані) механізми і змінні. При цьому під постійними розуміються такі механізми, які вбудовуються в компоненти КС у процесі створення СЗІ і перебувають у робочому стані весь час функціонування відповідних компонентів КС. Змінні механізми є автономними, використання їх для вирішення завдання захисту інформації передбачає попереднє здійснення операцій щодо введення їх до складу компонентів КС. Як вбудовані, так і змінні механізми можуть мати у своєму складі технічні, програмні й організаційні засоби забезпечення захисту. Механізми загальної організації роботи СЗІ призначені для системного узгодження та координації роботи всіх компонентів СЗІ.

Висновок. Для вирішення завдань захисту інформації в КС має бути включена система управління. Організаційно система управління складається з таких частин: механізмів забезпечення захисту інформації, механізмів управління ними і механізмів загальної організації роботи системи. У рамках концепції комплексної автоматизації система управління повинна охоплювати всі елементи КС. При цьому основні обов'язки щодо забезпечення необхідної ефективності захисту лягають на службу захисту інформації. Система управління повинна бути гнучкою, легко адаптуватись до конкретних умов, що складаються в процесі її цілеспрямованої діяльності. Інакше кажучи, завчасно повинні не просто визначатися конкретні рішення, а формуватися якомога більш повна технологія управління.

Список використаної літератури

1. Про затвердження Програми розвитку телекомунікаційної мережі та інформатизації ДПСУ на період до 2015 року : наказ Голови Держприкордонслужби від 05.05.2006 № 326.

2. Identity Finder Releases New Analysis of Stratfor/Anonymous Breach; Warns Victims to Beware of Phishing and Change Passwords http://www.identityfinder.com/blog/post/Update-Identity-Finder-Releases-New-Analysis-of-StratforAnonymous-Breach3b-Warns-Victims-to-Beware-of-Phishing-and-Change-Passwords.aspx

3. Герасименко В. А. Защита информации в автоматизированных системах обработки даннях / В. А. Герасименко. – М. : Энергоатомиздат, 1994. – Кн. 1, 2.

4. Терминология в области защиты информации : справочник. – М. : ВНИИ стандарт, 1993.

5. Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації : наказ Адміністрації Державної служби спеціального зв'язку

та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.2007 № 75/91. Зареєстровано в Міністерстві юстиції України 14.05.2007 за № 498/13765.

6. Про затвердження Правил посиленої сертифікації : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3. Зареєстровано в Міністерстві юстиції України 27.01.2005 за № 104/10384.

Рецензент – доктор військових наук,
старший науковий співробітник Кириленко В. А.

Стаття надійшла до редакції 14.01.2013.

Стрельбицкий М. А. **Декомпозиция технологии защиты информации в корпоративных системах**

В статье определены составные части комплексной системы защиты информации в корпоративных системах на стадии их модернизации. Приведены их три организационные части: механизмы обеспечения защиты информации; механизмы управления механизмами защиты информации и механизмы общей организации работы системы. Результатом исследования является представленная схема управления защитой информации.

Ключевые слова: *защита информации, корпоративные системы.*

Strelbitskyi M. A. **Decomposition of information security technologies in corporate systems**

The article defines the components of complex information security technologies for corporate systems at the stage of their modernization. Their three organizational parts have been given. They are the following: mechanisms of protection of information, mechanisms of management of tools of protection of information and mechanisms of general organization of system work. The result of research has become the scheme of management of information security.

Keywords: *information security, corporate systems.*