The II[nd]International Conference «Advanced Information Systems and Technologies, AIST 2013»
21-24 May 2013, Sumy, Ukraine

# Захист інформації від несанкціонованого доступу

Куліш А.М., Єрьоміна Марина Олександрівна
Сумський державний університет, юридичний факультет;
Доктор юр.наук, професор, декан юр. факультету; студентка гр. Юс-22
e-mail: m-eremina@mail.ru

***In this issue are considered shortcomings of the system information security and ways and methods of protecting information from unauthorized access.***

## ВСТУП

На сьогодні розвиток науки, технології не стоїть на місці. Зростає кількість інформації, яка обробляється, передається та зберігається в сучасних інформаційно-комунікаційних системах та мережах.Але зі зростанням кількостіінформації зростають і випадкинесанкціонованого доступу до неї. Тому метоюінформаційної безпеки як раз і є створенняперешкоднеконтрольованомурозповсюдженню даних, попередження їх втрати або відсутності доступу до них.

Для ефективного вирішення даної задачі необхідний аналіз усіх можливих способів та методівнесанкціонованого доступу до інформації в комп'ютерних системах, що дозволяє вчасно вжити заходів для протидії можливим загрозам. Несанкціонований доступ є реалізацією навмисної загрозиінформаційно-комп'ютерної безпеки, яка призводить до матеріальних втрат комп'ютерної мережі та порушує її ефективне і надійне функціонування [3].

## ОСНОВНИЙ ТЕКСТ

Основними причинами реалізації несанкціонованого доступу є недоліки сучасних інформаційних технологій, структури інформаційних систем та мереж, а також неухильний ріст складності програмно-апаратних засобів обробки і захисту інформації. У звязку з цим виникають загрози порушення конфіденційності, цілісності та основних властивостей інформації.Такі загрози можуть розрізнятися за способом їх реалізації. Джерелом ненавмисних загроз інформаційних систем можуть бути вихід з ладу апаратних чи програмних засобів, неправильні дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні та ін. Однак більш значними є навмисні загрози, які, на відміну від випадкових, мають на меті завдання збитків інформаційній системі або користувачам. Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами, тощо. Наслідками таких атак можуть бути і руйнування і втрата і зміна інформації на помилкову, а також ознайомлення з нею сторонніх осіб[3]. Серед недоліків систем захисту від несанкціонованих дій виділяють випадки коли відсутня гнучка система підтвердження користувачів при вході в комп'ютерну систему. Відповідно до цього адміністратор не має можливості вибору способу аутентифікації, тому що найчастіше система захисту включає тільки функцію підтвердження дійсності на основі простого пароля [1,с.77].

Якщо звернути увагу на порядок розмежування доступу в багатьох системах, то він не є надійним через відсутність діючих способів криптографічного захисту інформації. Крім того, більшість систем не забезпечує мандатного контролю доступу, а відповідно не дозволяє розмежувати комп'ютерні ресурси по рівнях таємності і категоріям. У ряді випадків відсутня можливість задання паролів по доступу до

окремих найбільш важливих комп'ютерних ресурсів.

Чунарьова А.В виділяє серед недоліків систем захисту від несанкціонованих дій також і захист від комп'ютерних вірусів. У більшості систем відсутній вбудований захист від комп'ютерних вірусів, що істотно знижує безпеку обробки і збереження даних. Зараження комп'ютера чи локальної мережі вірусом може привести як до втрати працездатності комп'ютерної системи, так і порушення цілісності і конфіденційності інформації, що зберігається в ній[3].

Недоліком сучасних систем безпеки є недостатньо висока швидкість криптографічних перетворень, що змушує користувачів відмовлятися від функції шифрування. Крім цього криптографічні засоби інформації які на сьогодні писутні на ринку не забезпечують належний рівень захисту від розкрадання інформації,її перетворення або навіть знищення.

Для того, щоб врегулювати та вирішити проблеми, які стосуються несанкціоновоного доступу до інформації,необхідно здійснити такі етапи:

1. Ретельний аналіз структури і принципів функціонування комп'ютерної мережі, що атакується, з метою пошуку уразливостей системи захисту її ресурсів.
2. Аналіз знайдених слабостей і розробка найбільш діючих способів подолання системи інформаційно-комп'ютерної безпеки.
3. Виконання підготовлених атак і оцінка отриманих результатів.
4. При невідповідності отриманих результатів необхідний ретельний аналіз процесу виконання атак і перехід до першого кроку для уточнення способів їхньої реалізації.

Після проведення необхідних аналізів можливе виялення проблеми та її вирішення, що покращить захист інформаційних систем та ресурсів. Але на сьогодні не існує "абсолютно надійних" методів захисту інформації, які гарантують повну неможливість отримання несанкціонованого доступу. Тому при захисті від несанкціонованого доступу слід виходити зприпущення, що рано чи пізно цей захист виявиться знятим. Метою захисту повинен бути вибір такого способу, який забезпечить неможливість отримання несанкціонованого доступу для заздалегідь визначеного кола осіб протягом обмеженого часу [2].

## ВИСНОВКИ

Отже, дослідивши способи несанкціонованого доступу можна визначити основні шляхи захисту інформаційних ресурсів, які допоможуть користувачеві захистити інформацію від несанкціонованого доступу.Такими шляхами є:

- Звертати увагу на безпеку контролерів домену, серверів, служб, додатків і підключень до Internet, оскільки у мережі існує велика кількість облікових записів адміністратора які при використанні можуть привести до несприятливих наслідків.
- використовувати контроль шифрованої файлової системи. Ця система є могутньою опцією для захисту даних, які знаходяться на компютерах. Шифрування допоможе захистити дані від користувачів або хакерів, що намагаються одержати до них доступ, але не спроможних розшифрувати ці дані.

## ЛІТЕРАТУРА


[1] Саврук М.В. Актуальність проблеми інформаційної безпеки в Україні та шляхи її розв’язання/М.В. Саврук//Системи обробки інформації.-2010.-№3(84).-С.77-79

[2] Чернявська Т.О. Шляхи захисту інформаційних ресурсів від несанкціонованого доступу [Електронний ресурс].- Режим доступу: http://www.rusnauka.com/13_NMN_2011/Informatica/4_85740.doc.htm

[3] Чунарьова А.В., Чунарьов А.В. Аналіз актуальних способів та методів несанкціонованого доступу в сучасних інформаційно- комунікаційних системах та мережах [Електронний ресурс].-Режим доступу: http://www.rusnauka.com/35_OINBG_2010/Informatica/76311.doc.htm