УДК 004.087.2

ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ З'ЄМНІ НОСІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Бєтанов Є.В. Петренко А.Б.
Національний Авіаційний Університет м. Київ

В роботі були проаналізовані канали витоку інформації в автоматизованих системах, а також сформоване завдання по створенню програмного продукту по захисту автоматизованих систем від підключення незареєстрованих пристроїв з інтерфейсом підключення USB. Також представлений опис продукту, що блокує USB порти при виявленні підключення зовнішнього пристрою, що не був попередньо занесений до спеціальної бази даних. Робота являється продовженням наукових трудів [3, 4].

Ціль системи захисту електронної інформації – зберегти такі властивості інформації як конфіденційність, цілісність, спостереженість, доступність та достовірність.

Всі загрози інформаційній безпеці можна поділити на внутрішні та зовнішні.

Як демонструє практика, найслабкішим місцем будь якої системи захисту, являються внутрішні загрози. Проведені дослідження з приводу співвідношення внутрішніх та зовнішніх загроз говорять про те що внутрішні загрози складають 57 відсотків від всіх загроз інформаційній безпеці.

Дії персоналу, що має безпосередній легальний доступ до автоматизованої системи, контролюються нормативними та організаційними заходами. Але при спробі здійснення несанкціонованого доступу їх буде замало.

Найуразливішим місцем будь-якої системи захисту являється користувач системи, що має безпосередній легальний доступ до своєї станції.

Користувач, що був автентифікований може спричинити наступні загрози: здійснити крадіжку конфіденційної інформації, порушити авторські права на інформацію, здійснити саботаж інформації,

Проаналізувавши можливості по утворюванню користувачами каналів витоку інформації, можна перерахувати їх в порядку зменшення імовірності реалізації[2]:

- зовнішні носії 45%;
- пересилання файлів мережею Internet 25%;
- друк файлів на принтері 13%;
- фотографування документів на цифрові камери 12%;
- інші 5%.

До реального здійснення попередження неправомірних дій з інформаційними ресурсами необхідно обмежувати автентифікованого користувача на здійснення підключення незареєстрованих з'ємних носіїв інформації.

Таким чином авторами була поставлена задача розробки програмного продукту, що обмежуватиме використання запам'ятовуючих пристроїв, і таким чином покращити систему захисту інформації в автоматизованих системах різного класу.

У запам'ятовуючих пристроях комп'ютерної системи, як правило, міститься інформація про конфігурацію системи[1]. До такої інформації відносяться: типи пристроїв та їх характеристики, кількість і особливості підключення зовнішніх пристроїв, режими роботи і інша інформація. Конкретний склад особливостей конфігурації визначається типом комп'ютерної системи і операційної системи. У будь-якому випадку, за допомогою програмних засобів може бути організований збір і порівняння інформації про конфігурацію комп'ютерної системи.

Ще більш надійним та оперативним методом контролю – використання спеціального коду-ідентифікатора пристрою. Цей код може генеруватися апаратними засобами, а може зберігатися в запам'ятовуючих пристроях. Генератор може ініціювати видачу в контролюючий пристрій (в обчислювальній мережі це може бути робоче місце адміністратора) унікального номера пристрою. Код

із запам'ятовуючого пристрою може періодично зчитуватися і аналізуватися засобами адміністратора комп'ютерної системи.

Було створено програмний продукт, що блокує зовнішні пристрої накопичування даних з інтерфейсом підключення USB.

Програмний продукт відстежує підключення зовнішніх носіїв, і при спробі підключення будь якого пристрою виконує наступні дії.

- Перевіряє чи є дозвіл на використання цього пристрою, у цього користувача.
- Якщо дозволу немає – блокує цей пристрій. Якщо дозвіл є, тоді дозволяє користувачу працювати з цим пристроєм.
- Блокування проводиться в два етапи: відключення пристрою, блокування USB портів.
- При блокуванні подається візуальний сигнал тривоги.
- Дає можливість розблокувати порти адміністратору системи за надання ним персонального паролю.

При розробці програми були реалізовані наступні елементи.

- Функція, що відстежує підключення та перевірку носіїв.
- База даних, де зберігаються ідентифікатори носіїв, якими дозволено користуватися.
- Система управління базою даних, що дозволяє додавати, видаляти чи редагувати інформацію про пристрої та їх власників.
- Система адміністрування, що не дозволяє не санкціоновано змінити базу даних, вимкнути програму, розблокувати порти.
- Додаткового захисту пристроїв паролями користувачів.

Алгоритм роботи програми складається з кількох базових етапів.

- Алгоритм моніторингу портів та перевірки підключених пристроїв.
- Алгоритми адміністрування.

Робота з базою даних можлива від прав адміністратора та від прав користувача. Робота адміністратора передбачає підключення нових пристроїв для їх занесення в базу даних. Таким чином, захист системи при роботі від імені адміністратора буде повністю відключений. При виході з нього, система автоматично поновить моніторинг портів.

Робота під правами користувача, визначає зміну персонального паролю на носії. Режим захисту при цьому буде включений. В загальному вигляді ці алгоритми можна представити блок схемами, на яких будуть представлена послідовність дій по забезпеченню функціонування цих етапів.

Висновки. Авторами було розроблено програмний продукт, що дозволяє зберегти важливу інформацію на робочих станціях від не санкціонованого копіювання самими користувачами. В ситуації коли користувач помилково, залишив ввімкнений комп'ютер, а потенційний зловмисник намагатиметься скопіювати важливі дані, програма також не дозволить йому це зробити.

Таким чином використання даного програмного продукту доцільне для захисту інформації в автоматизованих системах.

Отже, можемо сказати, що подальша робота над даною системою доцільна і значно покращить систему захисту електронної інформації від несанкціонованого копіювання.

Література

[1] Карасик И.Г. Программные и аппаратные средства защиты информации для персональных компьютеров – Компьютер-пресс., 1992, №3 с.37-46.

[2] Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.: ил.

[3] Бєтанов Є.В. Петренко А.Б. Дослідження вразливих місць системи захисту інформації при використанні eToken. – Защита информации. Сборник науных трудов НАУ. Выпуск 17. Киев, 2010 р. – 221-225 с.

[4] Бетанов Е.В. Противодействие потере информации через USB носители. – Збірник тез VIII Міжнародної-технічної конференції студентства та молоді «Світ інформації та телекомунікацій - 2010» Київ, 27-28 квітня 2011 р. – 77-78 с.