ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Юскович-Жуковська В. І., Соловей Л. Я.
Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука, Рівне, Україна

Використання в мережі Internet технології WWW надає користувачам доступ до неосяжних масивів інформації та її обробки. В інформаційному суспільстві мають місце злочини у сфері комп'ютерної інформації, яким притаманний міжнародний характер. Тому на сьогодні актуальними є протидія зловживанню інформаційними технологіями, безпека інформації в автоматизованих системах (АС) керування різноманітними процесами та запобігання несанкціонованим діям щодо інформації в АС.

Відповідно до Закону України «Про захист інформації в автоматизованих системах» об'єктами захисту є інформація, що обробляється в автоматизованих системах та програмне забезпечення, яке призначене для обробки цієї інформації, права власників цієї інформації та власників АС, права користувачів (рис. 1). Відповідальність за забезпечення захисту інформації в АС покладається на власника системи [1].

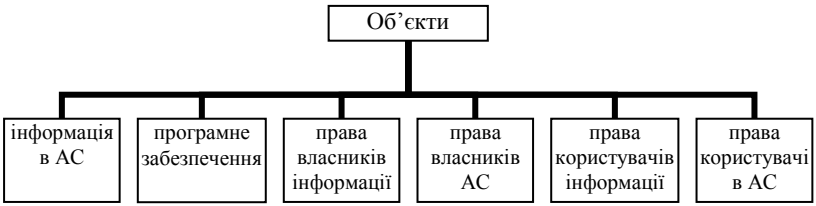

Рисунок 1 – Об'єкти захисту інформації в автоматизованих системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом [1].

Комп'ютерну злочинність та комп'ютерний тероризм в інформаційні сфері названо одними із загроз національним інтересам та національній безпеці України згідно ст.7 Закону «Про основи національної безпеки України». Об'єктами злочинних посягань являються саме відносини між суб'єктами у сфері комп'ютерної інформації [2].

Відносини між суб'єктами виникають в разі створення, зміни, збирання, накопичення, зберігання, пошуку, розповсюдження, використання, введення, копіювання, зчитування, знищення, реєстрації, а також: втрати, підроблення, спотворення, блокування інформації та інших неправомірних дій.

Комп'ютерна інформація являється одним з видів інформації, що має ознаки, які не властиві іншим видам інформації. Інформація - це основне поняття в кібернетиці. Серед комп'ютерних програм, з однієї сторони, є програми, які створені для захисту комп'ютерної інформації, з іншої сторони -

шкідливі програми, тобто віруси. Комп'ютерна інформація у сфері інформаційних відносин існує у формі електронного документу. Так, згідно Закону України «Про електронні документи та електронний документообіг» електронним документом є документ, інформацію в якому представлено у формі електронних даних, включаючи обов'язкові реквізити документа, зокрема й електронний цифровий підпис, який може бути сформований, переданий, збережений і перетворений електронними засобами у візуальну форму [3].

Обов'язковою ознакою електронного документа є електронний цифровий підпис. Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем. Суб'єкти електронного документообігу визначають режим його доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему захисту.

Безпека автоматизованої системи – це здатність АС забезпечувати конфіденційність і цілісність інформації від несанкціонованого доступу з метою її розкриття, зміни або знищення. Однією з основних інформаційних проблем XXI ст. вважають інформаційну безпеку даних. Це пов'язано з тим, що свідоме викрадення інформації, її спотворення і знищення призводить, як правило, до негативних наслідків для власників інформації, а іноді, навіть, до банкрутства фірми.

Рисунок 2 – Можливі загрози автоматизованим системам

Всі існуючі загрози автоматизованим системам можна умовно об'єднати у три групи: загрози розкриття інформації, загрози цілісності інформації, загрози відмови в обслуговуванні АС (рис.2).

Рисунок 3 – Класи методів інформаційної безпеки АС

Інформаційну безпеку АС забезпечують засоби, які можна умовно поділити на 4 класи: організаційні, технологічні, апаратні та програмні (рис. 3). Найрозповсюдженішими засобами захисту інформації в АС являються

програмні, наприклад, програми ідентифікації користувачів, парольний захист і перевірка повноважень, брандмауери, криптопротоколи та ін. Вартість ліцензійних програмних системних засобів по захисту інформації суттєво перевищує по затратах апаратні, технологічні, а тим більше організаційні засоби.

Розробники програмного забезпечення та його користувачі надають перевагу таким напрямкам захисту інформації в АС: захист від несанкціонованого доступу, захист таємної, конфіденційної та особистої інформації, захист АС від комп'ютерних вірусів (рис.4):

На сьогодні також активно розвиваються засоби захисту від витоку інформації по мережі Інтернет, засоби захисту від електронних «жучків», які встановлюються безпосередньо в комплектуючі комп'ютерів та ін.

Рисунок 4 – Напрями захисту інформації в АС

Світовій практиці відомі випадки здійснення хакерами витончених зв'язків з організованими злочинними угрупованнями, коли останні виступали в ролі замовників комп'ютерних махінацій, знімаючи через третіх осіб фінансові потоки в банківських комп'ютерних системах тощо.

Забезпечити повну безпеку інформації в автоматизованих системах практично неможливо, але знизити рівень ймовірності втручання шкідливих комп'ютерних програм – завдання цілком реальне. Для цього необхідно усунути обставини, що сприяли створенню, використанню та розповсюдженню шкідливих комп'ютерних програм.

Отже, безпеку інформації в АС можна забезпечити наступним чином:

1) дотримуватись норм, вимог, правил, щодо захисту оброблювальної інформації;

2) використовувати ліцензійне програмне забезпечення, сертифіковані засоби обчислювальної техніки, засоби зв'язку і АС в цілому;

3) здійснювати постійний контроль у реальному часі щодо захисту інформації в АС.

Список літературних джерел

1. Закон України «Про захист інформації в автоматизованих системах»

2. Закон України «Про основи національної безпеки України»

3. Закон України «Про електронні документи та електронний документообіг».