УДК 343.3/.7:004

О. С. Кульчицький, О. А. Ладигіна

Tigger100500@gmail.com, ladyginaoa@ukr.net

Центральноукраїнський національний технічний університет, м. Кропивницький

АНАЛІЗ РОБОТИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Безпека мережі – це заходи, які приймаються для захисту інформаційної мережі від спроб руйнування, втручання та неправомірних дій по відношенню до даної мережі.

Для забезпечення безпеки інформаційної мережі необхідно захистити дані, програмне забезпечення та обладнання, що використовується.

Усі дані в комп'ютерній системі можуть бути втрачені через розкрадання або несправність, так би мовити, "системних дир". Щоб захистити інформацію треба використовувати апаратні пристрої та засоби.

На даний момент часу є дуже багато способів розкрадання даних. Для отримання інформації не обов'язково підходити до того чи іншого комп'ютера та копіювати файли на флешку, як це робилось раніше. 2019 рік має можливість встановити пристрої, програми в комп'ютер або монітор для виводу шпіонажу на інший монітор чи клавіатуру.

Але не треба відразу "хвататись за голову" та панікувати, адже як вигадали таку загрозу для компаній, людей, так проти неї з'явились методи захисту:

1. Перешкоду можна створити програмними або фізичними засобами.

2. Криптографічні способи – перетворення інформації та її замаскування.

3. Спонукання, або створення умов, які будуть мотивувати користувачів ПК до належної поведінки та завжди дотримується правил поводження з даними.

Усі ці методи захисту будуть реалізуватися за допомогою організаційних та технічних засобів.

Розробка організаційних засобів захисту інформації відноситься до обов'язків служби безпеки:

1. Інструктаж та перевірки усього персоналу компанії.

2. Підписання додаткових угод до трудових договорів з відповідальністю за розголошення таємниць по роботі.

3. Розробка програм, які захищають дані від знищення або копіювання.

Технічні засоби захисту поєднують разом програмну та апаратну частину:

1. Завжди перед будь-якими діями не завадить зробити резервне копіювання даних.

2. З часом з'явилось дуже багато хмарних сервісів для зберігання даних.

3. Встановлення програмного забезпечення, яке захищає базу даних та іншу інформацію від незаконного доступу.

4. Ще можна встановити в офіс камери та сигналізацію разом з охороною аби не пролізли шахраї.

5. Найголовніша міра захисту комп'ютера від людини, яка не за того себе видає – пароль.

Безпечною дією безпеки є аутентифікація. Для неї необхідно знати ім'я користувача та пароль, щоб без перешкод зайти в свій запис.

Спосіб використання лише імені користувача називають аутентифікацією однофакторною. Коли користувач використовує мобільний зв'язок чи кредитну картку, то дана безпека має назву двофакторна аутентифікація. Ще є трьохфакторна аутентифікація, при якій використовується сканування сітківки ока, тобто сканер обличчя чи відбитки пальців. Після проходження даної перевірки, відкривається доступ до користування послуг мережі.

Щоб виявити шкідливі програми, або їх пригнічення, використовується антивірусне програмне забезпечення. Також може використовуватися система запобігання вторгнень. Якщо однією мережею користується декілька комп'ютерів, то зв'язок між ними зашифровується. Дані дії проводяться для дотримування конфіденційності від інших людей.

На підставі вище викладеної інформації можна зробити висновок, що існує декілька видів безпеки захисту роботи комп'ютерних систем та мереж. Кожна з них по-своєму має свої "за" і "проти" для використання в роботі. Тому, користувач або організація вибирає найбільш ефективні способи захисту своєї системи та мережі [3].

Список літератури

1. В. П. Мельников, С. А. Клейменов, и А. М. Петраков, "Информационная безопасность и защита информации", *Академия,* 2011.

2. Способы защиты информации, [Электронный ресурс]. Доступно: https://searchinform.ru. Дата обращения: Апрель 02, 2019.

3. О. С. Кульчицький, "Вимоги протидії кіберзлочинності в умовах громадської локалізації", *Комп'ютерна інженерія і кібербезпека: досягнення та інновації: матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених*, 2018.