Недоліки «Perenio» PECSS01:

- необхідне постійне підключення до мережі Інтернет;
- потреба у мобільному застосунку для налаштування;
- повідомлення приходить лише у додаток.

У даному докладі пропнується датчик диму на основі мікроконтролеру «Arduino Leonardo», який дозволяє уникнути перелічених недоліків та використовує наступні апаратні модулі:

- мікроконтролер «Arduino Leonardo»;
- датчик диму «MQ-2»;
- GSM модуль «SW M590E»;
- датчик звукового сповіщення «MH-FMD»;
- акумуляторна батарея.

Датчик диму на мікроконтролері «Arduino Leonardo» працює на основі газового сенсора «MQ-2», який при виявлені часток диму відправляє сигнал до мікроконтролер, якщо цей сигнал перевищує норму у 1000 PPM, «Arduino Leonardo» завдяки алгоритму увімкне звуковий сповіщувач та відправить SMS повідомлення на задані у алгоритмі номери телефону.

Переваги запропонованого рішення :

- датчик не потребує Інтернет-з'єднання;
- не потрібний мобільний додаток для його налаштування;
- можна працювати з будь яким типом мобільного пристрою (телефону);
- надійність приладу і системи;
- низьке електроспоживання пристрою.

Список використаних джерел:

1. WorldVision. URL: https://worldvision.com.ua/v-chem-raznitsa-mezhdu-ionizatsionnymi-i-fotoelektricheskimi-pozharnymi-datchikami/
2. Ajax. URL: https://ajax.systems/ru-ua/products/fireprotect/
3. Perenio. URL: https://perenio.ua/ru/catalog/datchik-dyma-pecss01-pecss01

Науковий керівник: доцент Бойко В. Д.

ЩОДО ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ, ЩО ЗБЕРІГАЄТЬСЯ НА КОМП'ЮТЕРАХ КОРИСТУВАЧІВ

Чанишев Р. І.

кандидат юридичних наук, доцент,
доцент кафедри інформаційних технологій,
Національного університету «Одеська юридична академія»

Незважаючи на всі заходи, що вживаються фахівцями із забезпечення комп'ютерної безпеки, витоки конфіденційних даних, що зберігаються в комп'ютерній формі, продовжують відбуватися досить регулярно навіть у найбільших IT-

компаній, таких, як Facebook, Apple, Amazon та ін. [1]. Ці витоки торкнулися і мільйонів українських користувачів. Так, у вересні 2021 року стало відомо про те, що хакери отримали доступ до майже 53 млн. записів з персональною інформацією українців [2].

Ситуація погіршилася в період пандемії COVID -19, коли багато компаній перевели своїх співробітників на режим дистанційної роботи. У цьому режимі працівники почали масово підключатися до корпоративних мереж зі своїх особистих персональних комп'ютерних пристроїв, значну кількість яких не підготували до роботи з конфіденційними даними. Протягом двох років пандемії компанії активно вживали заходів, що дають змогу забезпечити безпеку даних при підключенні віддалених користувачів, проте підсумкові результати виявилися невтішними. Так, компанією Check Point Software Technologies на початку 2022 року були представлені результати дослідження, проведені за участю 1200 фахівців з інформаційної безпеки та інформаційних технологій у всьому світі. За їхніми результатами, 20% компаній все ще не запровадили критично важливі засоби забезпечення безпеки під час віддаленої роботи [3].

Цей приклад є дуже показовим – із завданням забезпечення безпеки під час роботи з корпоративними даними на особистих комп'ютерах користувачів не змогли повноцінно впоратися й корпоративні спеціалізовані підрозділи, основним завданням яких є захист інформації, що в такому разі очікується від звичайних користувачів.

В умовах воєнного стану в Україні ситуація ще загострилася. Тепер дані, що зберігаються на персональних комп'ютерних пристроях користувачів, можуть потрапити в руки ворога і використовуватися противником у своїх цілях. Причому їм може бути використана будь-яка інформація, виявлена на пристрої, включаючи і ту, що у мирний час не була конфіденційною чи секретною. Особливістю поточного моменту є те, що шанси отримання безпосереднього доступу до самого комп'ютерного пристрою (а не тільки віддаленого через мережу) у противника збільшилися на порядок. Особливої гостроти цієї ситуації додає можливість втрати користувачем своїх комп'ютерних пристроїв під час вимушеної евакуації, і, як наслідок – влучення цих пристроїв у чужі руки.

Виходячи з вищевикладеного, безумовно, є необхідним вживання термінових заходів щодо безпеки особистих комп'ютерних пристроїв. Крім уже відомих заходів, таких, як використання тільки легального пропрієтарного або вільно розповсюджуваного програмного забезпечення, обов'язкового використання антивірусних програм та своєчасного резервного копіювання, необхідно використовувати і додаткові. До таких, наприклад, можна віднести використання хмарних технологій та шифрування дисків комп'ютера.

Навіть безкоштовний особистий обліковий запис, отриманий у одного із західних провайдерів хмарних технологій, дає можливість розмістити у хмарному сховищі до 5 гігабайт файлів. Цього обсягу цілком вистачає для збереження великої кількості файлів текстових документів, табличних даних, документів у

форматі Word чи Excel. При платному доступі доступні сховища обсягом від одного терабайта та вище, що дозволяє зберігати у хмарі графічну та відео інформацію.

Важливість хмарних технологій повною мірою змогли оцінити люди, які змушені терміново змінити своє місце проживання або евакуюватися. Дані, збережені в хмарному сховищі, залишилися для них доступними навіть з огляду на те, що їхні особисті комп'ютери залишилися в інших містах. Крім того, дані, збережені в тільки хмарі, будуть недоступні для сторонніх осіб, які вирішили скористатися чужими комп'ютерами, що потрапили в їхні руки.

15 березня 2022 року Верховна Рада України прийняла за основу та в цілому Закон «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» за №7152.

У проекті Закону зазначається, що «власники системи для забезпечення належного функціонування систем та захисту інформації, що обробляється в них … забезпечують створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх зберігання, у тому числі за межами України … можуть розміщувати державні інформаційні ресурси та їх резервні копії на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування».

Додатково у проекті Закону зазначається, що: «Забороняється ведення публічних електронних реєстрів, за допомогою хмарних ресурсів та/або центрів обробки даних, що розміщені на території України, де органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та територіях держав, які входять до митних та воєнних союзів з такими державами» [4].

Шифрування дисків комп'ютера при використанні операційних систем сімейства MS Windows (починаючи Windows 7) може бути здійснено за допомогою входить до комплекту постачання професійної версії цієї операційної системи програми BitLocker.

Шифрування дисків за допомогою BitLocker можна проводити як на комп'ютерах із вбудованою (або додатково встановленою) апаратною підтримкою шифрування за допомогою модуля TPM (Trusted Platform Module), так і на комп'ютерах без апаратного TPM. При цьому можна шифрувати і окремі логічні диски (включаючи системні диски і диски з даними), на які може бути розбитий фізичний накопичувач комп'ютера. Крім того, за допомогою BitLocker можуть бути зашифровані і зовнішні накопичувачі, такі, як USB флеш-накопичувачі та зовнішні жорсткі диски.

Можливість шифрування дисків на комп'ютерах, де апаратний модуль TPM не встановлено, забезпечується тим, що ці сучасні процесори здатні програмно емулювати роботу апаратного модуля TPM. При цьому на багатьох старих материнських платах (розроблених ще до виходу Windows 11) необхідно включити підтримку як апаратного, так і програмного TPM в BIOS комп'ютера.

При запуску комп'ютера, системний диск якого було зашифровано за допомогою програми BitLocker, у разі використання старих материнських плат потрібно ввести пароль на сам BitLocker. У нових системах достатньо ввести пароль (або пін-код) тільки на вхід до системи Windows. У разі підключення зовнішнього накопичувача, зашифрованого за допомогою BitLocker, необхідно ввести пароль для розблокування. У тих випадках, коли користувач забув пароль до диска, зашифрованого за допомогою BitLocker, доступ до накопичувача можна отримати за допомогою ключа шифрування, який можна зберегти не тільки в письмовому вигляді, а й у хмарному сховищі (що є найбільш безпечним та зручним варіантом збереження) .

Зловмисник, який одержав фізичний доступ до комп'ютера, не зможе увійти в систему, не знаючи пароля. Якщо ж накопичувач буде вилучено з комп'ютера – прочитати дані на іншому пристрої з цього накопичувача неможливо.

На комп'ютерах, вироблених корпорацією Apple, що працюють під керуванням операційної системи macOS, аналогічні функції шифрування диска виконують програма FileVault та апаратний модуль Apple T2 Security Chip.

Як видається, шифрування за допомогою таких програм є досить надійним. Однак, як було зазначено вище, доступ до зашифрованого диска можна отримати після введення пароля (або пін-коду) Windows. А такий пароль чи пін-код можна отримати від користувача методом соціальної інженерії чи просто підібрати його. За наявності фізичного доступу зловмисника до комп'ютера такий злом навіть за наявності шифрування диска за допомогою BitLocker/FileVault стає питанням часу. З цієї причини реальний захист може забезпечити лише фізичне видалення накопичувача з комп'ютера, наприклад, перед терміновою евакуацією. Зчитати інформацію із зашифрованого накопичувача без того комп'ютера, на якому його було встановлено, буде практично неможливо.

Але з видаленням накопичувача пов'язана ще одна проблема - конструкція комп'ютера повинна дозволити користувачеві зробити швидке вилучення накопичувача без руйнування конструкції комп'ютера. Однак більшість ноутбуків і моноблоків мають конструкцію, що дозволяє розібрати комп'ютер тільки в умовах майстерні.

З урахуванням вищевикладеного, можна дати такі рекомендації: при покупці основного робочого комп'ютера слід врахувати можливість виникнення необхідності самостійного вилучення накопичувача; файли, які є конфіденційними або можуть бути такими в умовах надзвичайного або військового стану, слід, по можливості, зберігати в хмарному сховищі; диски комп'ютера повинні бути зашифрованими, а у разі використання ноутбуків або моноблоків, всі файли,

створені особисто користувачем і які не зберігаються в хмарному сховищі, необхідно зберігати на зашифрованому зовнішньому жорсткому диску. Крім того, користувач повинен мати необхідний рівень знань для роботи із програмами шифрування дисків та окремих файлів.

Список використаних джерел:

1. Nearly 26M Amazon, Facebook, Apple, eBay user logins stolen by hackers. URL: http://surl.li/bzmzi
2. Устимович Ю. Масштабная утечка данных: хакеры «слили» почти 53 млн записей с персональной информацией украинцев. URL: https://thepage.ua/news/masshtabnaya-utechka-dannyh-hakery-slili-dannye-ukraincev
3. Check Point: большинство организаций до сих пор не обеспечили защиту удаленных сотрудников. URL: https://ko.com.ua/check_point_bolshinstvo_organizacij_do_sih_por_ne_obespechili_zashhitu_udalennyh_sotrudnikov_140240
4. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Проект Закону України №7152 від 13.03.2022. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39215

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ

Чеснок Б. О.

студент 1-го курсу факультету міжнародно-правових відносин Національного університету «Одеська юридична академія»

Право на захист персональних даних та недоторканність приватного життя є одним із основних прав людини. Зі швидким розвитком цифрових технологій та Інтернету це право було серйозно підірвано.

Час, коли ми живемо, так звана «ера великих даних», характеризується обробкою величезної кількості різноманітних даних. Наша особиста інформація розглядається як «нова нафта». Компанії фактично стягують плату з клієнтів за свої «безкоштовні» послуги, просячи їх залишати все більше особистих даних. Ну, всі ми знаємо стару приказку: «Безкоштовних обідів не буває». Інформація про користувачів, їхню діяльність та поведінку в мережі Інтернет використовується для: аналізу та створення особистих соціально-психологічних профілів; цільове розміщення комерційних продуктів з урахуванням індивідуальних особливостей та потреб користувачів (так званий one-to-one marketing) тощо.

Діти, будучи наймолодшими користувачами Інтернету, опинилися в центрі ринку персональних даних, що постійно зростає. Особи, які не досягли 18 років (діти) відповідно до чинного законодавства також належать до суб’єктів відносин, пов'язаних із персональними даними.

Згідно зі ст. 4 Закону України «Про захист персональних даних» суб'єктами відносин, пов'язаних із персональними даними, є суб'єкт персональних даних;