диск до обраної Live CD системи та безперешкодно копіювати данні з дисків, та в окремому випадку з під root, редагувати їх.

Роблячи підсумки, слід зазначити, що для захисту приватності інформації достатньо встановити пароль до BIOS, не використовувати емуляцію Legacy на Uefi Bios, завжди тримати увімкненим Secure Boot та зашифрувати данні за допомогою BitLocker.

Ці дії не уявляють складнощів та не заважають комфортному використанню пристроїв власником. Захистити данні від монтування або звичайного підключення до іншого комп'ютера диску можна завдяки пропрієтарній Windows програмі BitLocker, що зашифрує наявну інформацію на диску.

Список використаних джерел:

1. Яка різниця між UEFI и Legacy BIOS? /gravitsapa.info: веб-сайт. URL: https://gravitsapa.info/kakie-otlichiya-mezhdu-uefi-i-legacy-biosami/ (дата звернення 12.11.2021)

УДК 339.92

БАРАНЕНКО ЄГОР ОЛЕКСАНДРОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

заст. декана факультету з навчально-методичної роботи факультету №4

Харківського національного університету внутрішніх справ

БЛОКЧЕЙН, ЯК ВАРІАНТ ЗАХИСТУ ДАНИХ

З кожним днем роль кіберпростору в нашому житті невпинно збільшується. Щороку об'єм інформації в інтернеті зростає в рази, а з ним зростає кількість конфіденційної інформації, яку необхідно захищати.

Блокчейн перетворює цифрову ідентифікацію на реальність та допомагає захиститися від крадіжки ідентифікаційної інформації. Цифрова ідентичність - це інформація, яка зберігається в цифровому форматі і сама по собі є повним ідентифікатором. Користувач, за запитом та за своєю згодою, ділиться цією інформацією з організацією. Зацікавлена організація звіряє отриманий хеш із публічним репозиторієм хешів, наприклад, Aadhaar.

Хеші.

В основі блокчейну лежить обчислення математичного алгоритму хеша від заданого набору даних. Ось деякі властивості та особливості хешу:

- Хеш - це деяка кількість певної довжини;
- Хеш може бути отриманий в результаті перетворення даних на цифровий відбиток, тобто перетворити цілу енциклопедію на набір символів фіксованої довжини;
- Використовуються захищені алгоритми хешування, наприклад: SHA256, SHA384 та SHA512.
- З обчисленого хеша важко або неможливо отримати вихідні дані, навіть знаючи алгоритми, за якими формувався хеш.

У чому взагалі сенс блокчейн-безпеки, які її «населяють»? Технологія дозволяє людям, які не довіряють один одному, ділитися цінними даними безпечним та захищеним способом. Завдяки їй досягається:

- Блокування крадіжки особистих даних;
- Блокування підробки даних;
- Блокування DDoS-атак.

Якщо хеш збігається, це говорить про те, що посвідчення використовується автентифікованою особою. Дані помітні не завжди і знаходяться в захищеному вигляді до моменту перевірки.

Блокчейн замінює секретність на прозорість, розподіляючи докази підписання документа по багатьох блокчейнах. Практично неможливо маніпулювати даними.

Перевірка ідентичності без цифрового підпису – при цьому хеші вихідних файлів зберігаються у блокчейні, виконується перевірка інших копій файлів за допомогою алгоритму хешування та порівнюється результат із хешами, що зберігаються у блокчейні.

У *Hyperledger*, який є приватним блокчейном, існує мережа, в якій всі учасники заздалегідь відомі, а нові учасники перевіряються сертифікуючими органами перед підключенням. Є незначні шанси на DDoS-атаку, але всі учасники вже відомі винуватця буде легко виявити.

DoS і **DDoS** - це атаки, при яких на сервер приходить величезна кількість запитів, що сміття, що значно збільшує час відповіді сервера для відповіді на нормальні запити. У контексті *Ethereum* за будь-який запит, що обслуговується, повинна бути виплачена певна сума у вигляді *GAS* (найменша форма *Ethereum*). Такий підхід за своєю концепцією виключає DDoS-атаку.

Маніпуляції з даними будуть швидко виявлені, оскільки вихідний хеш існує на мільйонах вузлів.

Зазначимо, що міністерство оборони США розглядає блокчейн-інфраструктуру KSI як потенційно придатну для захисту чутливих військових даних. А ще існує компанія під назвою Gem, яка допомагає використовувати блокчейн для безпечного обміну медичними даними між зацікавленими сторонами відповідно до вимог американської HIPPA.

Блокування DDoS-атак.

Розподілені атаки типу «відмова від обслуговування» (DDoS) – це проблема, яка за умовчанням виключена у блокчейні. Давайте розглянемо це в контексті *Ethereum* і *Hyperledger*, обидві технології є різними формами блокчейна — публічний і приватний блокчейн відповідно.

Підбиваючи підсумки:

Зараз, запровадження блокчейн мереж може багатократно підвищити ефективність захисту даних користувачів, в порівнянні з сьогочасними методами. Ці мережі необхідно додаткового дослідити заради їх покращення та з’ясування можливості запровадження їх в сучасних реаліях сьогодення.