Ільєнко А. В., канд. техн. наук, доцент,
Ільєнко С. С., канд. техн. наук, доцент,
Куліш Т. М.
Національний авіаційний університет

ПРОГРАМНИЙ МЕТОД ЗАХИСТУ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS НА БАЗІ ТЕХНОЛОГІЇ BLOCKCHAIN

Щоденний обмін інформацією між користувачами і веб-сторінками вимагає підвищених вимог щодо захищеної передачі даних призначених для користувача. У сучасних умовах виникає необхідність розгляду нових методів і підходів для захисту операційної системи Windows [1-4]. Аналіз вразливостей, що і досі існують і усуваються патчами Microsoft підтверджують наявність недоліків у системі. Дуже актуальним являється питання поєднання традиційних способів захисту операційної системи з новітньою технологією Blockchain. Технологія Blockchain при використанні в сучасних інформаційних системах та мережах направлена на підвищення рівня цілісності і конфіденційність не тільки даних, а транзакцій між користувачами мережі при використанні операційної системи Windows. Наразі Blockchain набирає обертів, уже існують приклади використання даної технології у перевірці цифрових сертифікатів, але перевірка і досі не є повністю інтегрована із системою захисту Windows.

Метою даних досліджень є висвітлення перспективних методів захисту операційної системи Windows, окреслення основних підходів щодо забезпечення безпеки та визначення нових підходів до забезпечення безпеки операційної системи, а також представлення власної реалізації напрямку Blockchain для захисту Windows реалізованої мовою програмування Python 3.0 з подальшою можливістю її інтегрування в операційну систему.

На сьогодні вразливості в ОС можуть бути наслідком: програмних помилок (унаслідок помилки в програмному коді можна дозволити комп'ютерному вірусу отримати доступ до пристрою та взяти під контроль); довантажених функцій, патчів; неправильного налаштування і адміністрування ОС [2, 5].

Розглянемо деякі з вразливостей, виявлені у 2020 році. 14 січня 2020 року Microsoft випустила виправлення програмного забезпечення для вирішення 49 вразливих місць у рамках щомісячного оголошення Patch Tuesday. Серед виправлених вразливостей були критичні недоліки в Windows CryptoAPI, шлюз віддаленого робочого столу Windows (RD Gateway) та клієнт віддаленого робочого столу Windows. Зловмисник може віддалено використовувати ці вразливості для дешифрування, зміни або введення даних на з'єднання користувачів. До найбільш поширених вразливостей відносяться**:** вразливість підробки CryptoAPI (CVE-2020-060) **та** вразливості клієнта шлюзу Windows RD та віддаленого робочого столу Windows (CVE-2020-0609, CVE-2020-0610 та CVE-2020-0611). Для виявлення загроз та вразливостей операційної системи Windows використовуються популярні підходи і методи, а саме використання вбудованих засобів захисту програмного забезпечення, захист Active Directory, віртуалізація для стримування атак Подальші напрями дослідження Microsoft спрямовані на пошук перспективних методів захисту операційної системи Windows.

Доволі новим підходом, що має перспективу на використання для захисту Windows продуктів є використання Blockchain напрямку. Наразі він використовується для перевірки цифрових сертифікатів і можна однозначно сказати, що має потенціал і у інших напрямках забезпечення безпеки операційної системи. Дана технологія несе у собі підвищення рівня цілісності і конфіденційність не тільки даних, а транзакцій між користувачами мережі. Внесок цього напрямку значно підняв би рівень безпеки продукту Microsoft [2].

Blockchain це безперервний послідовний зв'язний список, побудований за певними правилами. Blockchain-розробник створює програмні додатки, які будуть виконуватися вузлами, що входять в ланцюжок блоків. Також він налаштовує взаємодію «класичного» програмного забезпечення, або DApp (Distributed application), з цими додатками. Авторами в ході дослідження запропоновані власні реалізації Blockchain для перевірки сертифікатів операційної системи Windows, враховуючи деякі із варіацій перевірок. Приклади реалізовано на Python 3.0.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гордеев, А.В. Операционные системы : учебник для вузов, Питер, 416 с., 2008.
2. Проскурин, В.Г. Защита в операционных системах, М. : Радио и связь, 192 с., 2014.
3. Дейтел, Х.М. Операционные системы. Ч. 2: Распределенные системы, сети, безопасность, М. : Бином, 704 с., 2006.
4. Дейтел, Х.М. Операционные системы. Ч. 1: Основы и принципы, М. : Бином, 1024 с., 2007.
5. Советы Microsoft [Онлайн] Режим доступу: https://www.cnews.ru/news/top/2020-0113_microsoft_predlozhila_400_mln_polzovatelej [21 березня 2021].