АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ВИБОРУ МЕТОДІВ БЕЗПЕЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ. ШИФРУВАННЯ ЧИ ТОКЕНІЗАЦІЯ?

ЛИСЕНКО Сергій Олексійович - доктор юридичних наук, професор, ПрАТ «Вищий навчальний заклад «Міжрегіональна академія управління персоналом», завідувач кафедри правознавства Сєвєродонецького інституту

ORCID ID: https://orcid.org/0000-0002-7050-5536.

DOI 10.32782/EP.2021.4.6

У статті розглядаються подібності та відмінності між двома популярними криптографічними методами передачі інформації: шифруванням та токенізацією. Наголошено, що, приймаючи рішення вибору між методами захисту, слід враховувати ряд моментів, включаючи спосіб використання даних та ключовий життєвий цикл управління організацією.

У процесі дослідження автор наводить різні підходи до визначення понять «шифрування», «шифр», виокремлюючи їх спільну складову. Як основну ознаку шифрування пропонується розглядати використання криптографічних ключів для перетворення даних (чіткої інформації) з читабельної у нечитабельну (шифротекстову) форму. При цьому «дешифруванням» є зворотне шифрування, використання криптографічних ключів для перетворення зашифрованого тексту назад у його початковий «прозорий та зрозумілий» вигляд.

У процесі аналізу підходів до визначення поняття «токенізація», автор виокремлює як спільну рису те, що основним описом токенізації є використання криптографічного методу для заміни читабельного прозорого тексту іншим читабельним прозорим текстом.

Окрему увагу присвячено огляду спроб органів державної безпеки різних країн контролювати досліджувані методи захисту інформації або протидіяти їм. Автор згадує протистояння уряду США та компаній Apple і Facebook, використання владою Гонконгу особливостей функціонування додатку Telegram. При цьому автор у жодному разі не надає оцінку етичності та правомірності втручання органів державної влади у роботу корпорацій та їх продуктів, акцентуючи увагу виключно на технічних особливостях того чи іншого механізму захисту інформації.

Серед іншого, наведено відмінності між симетричним і асиметричним шифруванням, табличним і випадковим методами токенізації.

Ключові слова: інформація, інформаційна безпека, правове регулювання, блокчейн, шифр, шифрування, дешифрування, токенізація, детокенізація.

Обґрунтування актуальності теми дослідження

Останніми роками дедалі більше уваги суб'єктів господарювання присвячується проблематиці захисту інформації. Серед лідерів у сфері технологій захисту інформації наразі перебувають шифрування і токенізація. Ухвалюючи рішення щодо вибору між методами захисту, слід враховувати ряд моментів, включаючи спосіб використання даних та ключовий життєвий цикл управління організацією.

Поширення проблеми вибору між шифруванням та токенізацією обумовлено природними особливостями цих методів. Питання вибору між ними постає кожен раз, коли виникає потреба конфіденційного обміну інформацією та даними. І, на жаль, таке просте питання досить важко вирішити однозначно. Спеціаліст із захисту інформації буде починати свою відпо-

від зі слів: «це залежить…», що насправді є цілком раціональним з теоретичної точки зору, але, на жаль, взагалі не допомагає на практиці. Обидва методи знаходяться в домені технології блокчейну і характеризуються рядом схожих та відмінних рис. Цю статтю присвячено порівнянню обох методів у намаганні відповісти на дилему вибору між використанням шифрування та токенізації.

Аналіз досліджень і публікацій щодо обраної тематики

Незважаючи на зростання уваги фахівців до розвитку технологій блокчейну у світі, вітчизняна наукова спільнота тільки починає реагувати на зміни у суспільних відносинах, обумовлені їх активним впровадженням. Серед вітчизняних публікацій, що так чи інакше пов'язані з технологіями блокчейну, можна згадати праці таких науковців, як: О. Баранов [1], В. Варавка [2], А. Гурова [3], М. Кірпачова [3]. Однак, з огляду на високі темпи розвитку технологій блокчейну та хронічне відставання української науки і практики їх застосування від світових лідерів можна вести мову лише про зародження вітчизняної блокчейн-сфери.Тому в ході цього дослідження активно використовуються окремі ідеї та напрацювання зарубіжних дослідників блокчейну, таких як Джефф-Стейплтон [4; 5; 6] та Лютер Мартін [7]. Автор має на меті здійснити огляд технологій шифрування і токенізації на підставі аналізу їх особливостей.

Основний зміст дослідження

Варто відразу зазначити, що обидва методи захищають дані через конфіденційність, але не забезпечують цілісності та достовірності [4].

Перш за все визначимось із сенсом шифрування. Усі знають, що таке шифрування, або принаймні більшість мають уявлення про його технологію, однак, за іронією долі, серед теоретиків науковців та практиків існують дещо різні визначення цього поняття. У найбільш загальному вигляді шифрування – це процес кодування повідомлення чи інформації таким чином, що до нього можуть отримати доступ та ознайомитись із цим лише уповноважені особи. Для прикладу тракт наведені загальноприйнятні визначення шифрування із відомих джерел.

1 «Шифрування» – алгоритмічне (криптографічне) перетворення даних, яке виконується у посимвольній послідовності з метою одержання шифрованого тексту [8].

2. Шифрування – надання тексту не зрозумілим за допомогою механізму кодуванням [9].

3. Шифрування - це (оборотна) трансформація даних за допомогою криптографічного алгоритму для отримання шифротексту (тобто для приховування інформаційного вмісту даних) [10].

4. Шифр (франц. первісно — нуль, цифра, секретне писання, від араб.— нуль) — Код, значення складових елементів якого і правила їх використання (кодування) відомі обмеженому колу осіб — шифрувальникам або користувачам відповідних кодів. Застосовується для утаємничення певної інформації з метою її захисту від несанкціонованого доступу і використання, особами, а також для охорони приміщень, сейфів, сховищ тощо [11].

З іншої точки зору, шифром є серія перетворень, яка перетворює простий текст у шифротекст, використовуючи так званий «ключ» шифру.

Незалежно від того, яке із наведених визначень шифрування здається більш звичним або робить його розуміння найбільш комфортним, основним описом шифрування є використання криптографічних ключів для перетворення даних (чіткої інформації) з читабельної у нечитабельну (шифротекстову) форму. Однак це лише половина процесу передачі інформації. Другою половиною є її отримання і переведення з нечитабельної у читабельну форму.

Дешифрування – це зворотне шифрування, використання криптографічних ключів для перетворення зашифрованого тексту назад у його початковий «прозорий та зрозумілий» вигляд. При цьому існує два принципово різних підходи до шифрування та дешифрування. ***Симетричне***

шифрування використовує один і той самий секретний ключ для функцій шифрування та дешифрування, тоді як ***асиметричне*** шифрування використовує два різні ключі, відкритий ключ для шифрування та приватний ключ для розшифрування.

Під час використання симетричної функції розшифровки з шифротекстом і секретним ключем, для одного виходу чіткого тексту, потрібно встановити загальний ключ. Але коли задіяно кілька сторін, то задіюють ключові комбінації управління. Симетричне управління ключами задіюється для кількох сторін.

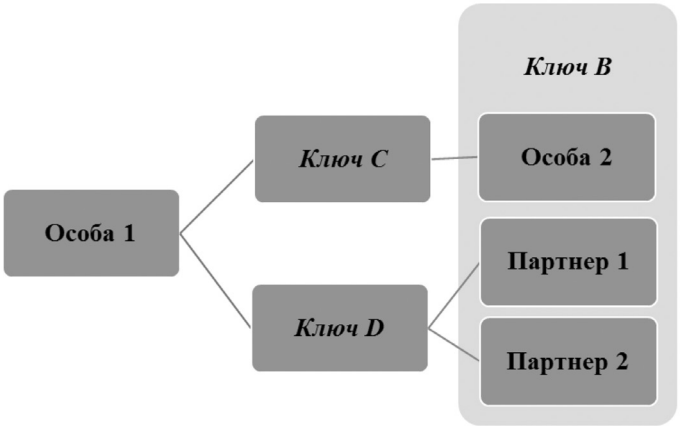

Рис. 1. Принцип дії симетричного шифрування

Припустимо, що Особа 1 (ліворуч) ділиться загальним «Ключем B» з кількома партнерами. Однак чіткий текст, зашифрований нею, може бути розшифрований всіма її партнерами, тому існує чітка відсутність конфіденційності. Особа 2 з (праворуч) може використовувати також «Ключ C», тоді як інші партнери (праворуч) використовують «Ключ D». У такому випадку, чіткий текст, зашифрований особою 1, може бути розшифрований основною Особою 2 (праворуч) сторони, але не іншими її партнерами (Рис. 1). Тим не менше, Особа 1 повинна керувати симетричним ключем для кожної сторони (ключі B,C,D), що не є особливо масштабованим. Натомість, асиметрична криптографія може зменшити кількість ключів, якими потрібно керувати.

Відкриті ключі можуть використовуватися як ключі шифрування даних або ключі шифрування ключів для управління іншими ключами. Особі 1 потрібно підтвердити, що це відкритий ключ прагне до Особи 2. Загальнодоступними ключами зазвичай керуються за допомогою цифрових сертифікатів, які підписуються та видаються від сертифікаційного органу, який працює у межах інфраструктури відкритих ключів, але таке обговорення [12] виходить за межі цієї статті.

Наразі, у повсякденному житті дедалі частіше зустрічається наскрізне шифрування. Іноді, коли користувачі починають новий чат і месенджер вітально повідомляє: «Дзвінки та повідомлення в цьому чаті тепер захищені наскрізним шифруванням», не всім зрозуміло про що йде мова. Простими словами наскрізне шифрування можна пояснити тим, що дзвінки, повідомлення, відео, аудіо, зображення, документи та інші дані доступні тільки двом співрозмовникам, тобто захищені від попадання в треті руки. Ключі шифрування є також тільки у них. За допомогою лише цих ключів можна розблокувати і прочитати повідомлення.

У кожного приватного чату є свій код безпеки, який використовується для підтвердження наскрізного шифрування повідомлень. Його можна знайти в розділі «Дані контакту» у вкладці «Шифрування» у вигляді QR-коду або 60-значного номера. Код безпеки – це видима версія спеціального ключа. Повна ж версія ключа зазвичай тримається в секреті. Крім того, кожне відправлене повідомлення має індивідуальний замок і ключ. Усе це відбувається автоматично і користувачам не потрібно нічого налаштовувати.

Популярність наскрізного шифрування особливо зросла в 2013 році, після того як Едвард Сноуден опублікував документи, які доводили, що уряд США відстежує кожен дзвінок і відправлене повідомлення. Після цього технологічні гіганти, такі як Apple і Facebook, вважали за краще убезпечити приватне життя своїх користувачів і ввели наскрізне шифрування[13].

За словами Олександра Огнєва, розробника курсу Skillbox з інформаційної

безпеки, існує два основних способи шифрування даних. «Симетричні криптосистеми мають на увазі, що для шифрування і дешифрування застосовується один і той же криптографічний ключ. Щоб забезпечити стійкість криптосистеми від злому, до даних застосовуються алгоритми, необхідні для захисту. Іншими словами, самого ключа недостатньо, необхідно перемішати дані таким чином, щоб забезпечити надійність. Однак при наявності досить великих продуктивних потужностей ключ можна підібрати. Щоб вирішити цю проблему, фахівці безпеки збільшують такі параметри, як довжина ключа, складність і число раундів перетворення»[14].

Уже згадувався вище інший підхід до шифрування даних – асиметричне шифрування. Для захисту даних використовуються два ключі – відкритий і закритий. Відкритий потрібен для зашифровуваних даних, при цьому вже для розшифровки він абсолютно незастосовний. З цієї причини він доступний усім, хто хоче спілкуватися з хранителем закритого ключа. І тільки за допомогою останнього можна розшифрувати дані. «Наскрізне шифрування може комбінувати ці два методи.- У випадку з месенджерами, ключі локалізовані каналом зв'язку і відомі тільки тим, хто спілкується між собою. Таким чином, дані, які може перехопити зловмисник, будуть марні», – пояснює Огнєв [14]. Відтак, ключовою характеристикою месенджерів, що використовують наскрізне шифрування, є приватність і анонімність. Під приватністю даних мається на увазі, що ніякі дані не доступні третім особам. Характерно, що у популярних месенджерів є певні напрацювання в цьому напрямку. Наприклад, Telegram має функцію самознищення акаунта в разі відсутності активності користувача.

Як доволі слушно зазначає Огнєв, анонімність месенджерів виражається в тому, що зв'язок встановлюється через сервери компанії, і учасникам спілкування не відомі IP-адреси віддаленого опонента. Але технології зв'язку, реалізовані в клієнтах, можуть мати свої недоліки. Наприклад, у WhatsApp при інтернет-дзвінках була можливість розкриття реальної IP-адреси користувача навіть без встановленого сеансу зв'язку[13]. При цьому, недоліком усіх месенджерів лишається авторизація за номером стільникового телефону. Спецслужби багатьох країн мають доступ до обладнання стільникових провайдерів зв'язку і можуть відправляти SMS із чужого номера без будь-яких повідомлень. А власник про це навіть не дізнається.

Прецедент мав місце у 2016 році, коли ФБР намагалося змусити Apple розкрити дані, що зберігаються в телефоні одного зі злочинців, які влаштували масову стрілянину роком раніше в Сан-Бернардіно. Гендиректор Apple Тім Кук заявив, що не збирається виконувати прохання ФБР, оскільки, на його переконання,«це розв'яже уряду руки, і він відчує, що може вести агресивну політику щодо втручання в приватне життя громадян [15].Така ситуація не могла влаштувати органи безпеки, і вже у вересні 2019 року за угодою між Лондоном і Вашингтоном американські соціальні медіаплатформи, у тому числі Facebook і WhatsApp, зобов'язали передавати зашифровані повідомлення користувачів поліції Великобританії для надання допомоги при розслідуваннях щодо осіб, підозрюваних у серйозних злочинах [16]. А в кінці листопада 2019 року Міністерство юстиції США заявило, що збирається почати масштабне розслідування щодо технологічних гігантів через те, що ті не надають уряду і силовим відомствам доступ до листування користувачів [17]. Однак навіть у таких умовах, у грудні 2019 Facebook відхилив прохання влади США відмовитися від наскрізного шифрування, завдяки якому перехоплювати повідомлення стало неможливо [18].

Улітку 2019 року, у ході протидії масовим протестам, влада Гонконгу задіяла метод стеження за користувачами Telegram. При додаванні номера телефону в контакти цей месенджер зіставляє введені дані з профілем користувача [19]. Тобто додавання номеру людини у вашу записну книжку дає змогу написати їй повідомлення. Саме цим скористалася влада Гонконгу для встановлення осіб протестувальни-

ків. Як стверджує Олександр Огнєв, тоді були створені спеціальні групи, які методом перебору додавали протестувальників у свої контакти і зіставляли їх з реальними людьми[13]. Звісно ж, цей метод є доволі кустарним, і характеризується рядом недоліків, зокрема – вимагає великих людських ресурсів і часу. Однак, сам факт можливості використання такої технології є яскравим свідченням значення та ролі шифрування.

Надійним критеріям інформаційної безпеки можуть відповідати також кілька менш відомих рішень. Одним із таких прикладів є месенджер Briar, ключовими особливостями якого є можливість з'єднання через Bluetooth або WI-FI, безпосередньо між пристроями, а також через мережу «Tor» [20]. Крім цього, з'єднання можливо без централізованих серверів, а відповідний контент зберігається в зашифрованому вигляді на пристроях учасників.

Тепер варто розглянути інший спосіб криптографічної передачі інформації – токенізацію. Так само, здається, кожен знає, що таке токенізація, або, принаймні, має свою думку. Залежно від домену програми, токенізація насправді може мати дещо різні значення.

Подібно до шифрування, токенізація має кілька визначень.

1. Токенізація при застосуванні до захисту даних – це процес заміни чутливого елемента даних на нечутливий еквівалент (що називається *токеном*), який не має зовнішнього або експлуатованого значення.

2. Токенізація: процес відображення значення простого тексту до дійсного або новоствореного сурогатного значення [12].

3. Токенізація – це процес, за допомогою якого основний номер рахунку (PAN) замінюється сурогатним значенням, що називається маркером. Варто зауважити, що це визначення є специфічним для стандартів токенізації платіжних карток (PCI) [21; 22; 23].

Незалежно від того, яке визначення токенізації здається більш звичним або здається читачу найбільш комфортним, основним описом токенізації є використання криптографічного методу для заміни читабельного прозорого тексту іншим читабельним прозорим текстом. Це аналогічно старомодним кодам, у яких використовувалася заміна слів.

Наприклад, шпигун може повідомити про «три качки та двох жаб у ставку», але прихований сенс повідомлення буде містити «три есмінці та два підводні човни в гавані». Тобто головна мета токенізації – уникнути розкриття конфіденційних даних за допомогою лексем.

Функція токенізації має два методи, прозорий текст та методологію маркера, і один вихід. Кожен з методів більш детально описаний далі. ***Випадковий метод***: використовує генератор випадкових чисел (RNG) для генерації випадкового значення для маркера. ***Табличний метод***: використовує генератор (RNG) та псевдовипадкових чисел (PRNG) для генерації статичної таблиці, що використовується для генерації лексем.

Функція детокенізації має два методи, методологію токена та лексеми, і один вихід, чіткий текст. Випадковий метод: чіткий текст не може бути відновлений з маркера, оскільки вони не мають визначеної кореляції. Метод таблиці: обернена функція використовується для відновлення прозорого тексту з маркера.

Метод розшифровки використовує симетричний ключ для розшифрування маркера та відновлення прозорого тексту. Прозорий текст неможливо відновити з маркера, оскільки він не надає достатньої кількості даних для отримання тексту.

Слід зауважити, що методологія Random та MAC не може використовуватися для детокенізації. Окрім того, деякі рішення токенізації використовують більше одного методу. Наприклад, гібридна токенізація може використовувати певну таблицю з методами шифрування для токенізації та дешифрування за допомогою методів зворотної таблиці для детокенізації.

Отже, шифрування – це визнаний метод токенізації, який додає плутанини. Крім того, деякі рішення для токенізації включають шифрування формату (FPE) [24].-

FPE не є власне криптографічним алгоритмом, скоріше це режим роботи, який використовує дійсний алгоритм шифрування (наприклад, AES) із чітким текстом і симетричним ключем як входи, але його шифротекст підтримує довжину і набір символів, як чіткий текст.

Наприклад, якщо шести цифрове число зашифроване за допомогою FPE, на виході отримується ще одне шестицифрове число. При цьому, режими FPE є оборотними, щоб шифротекст можна було розшифрувати.

Варто зазначити, що додатки можуть мати загальні токенізовані дані, які потрібно детокенізувати, але це ставить під загрозу все середовище онлайн-сервісу. Кожен раз, коли детокенізується маркер, він збільшує ймовірність зловживань або компрометації системи токенізації.

Як порівняння, спільність шифрування полягає в тому, що прозорий текст обробляється програмою. Токенізація призначена для захисту даних у сховищі або під час їх обробки. Для безпеки маркери зберігаються на диску, зчитуються та обробляються виключно програмою. При цьому, маркери передаються, приймаються та обробляються додатком.

Методи шифрування, як правило, використовують однакові алгоритми для надійності та спрощення реалізації, але різні криптографічні ключі зміцнюють загальну безпеку. Однак програми, що покладаються на токенізацію, потребують однаковості, тому алгоритми повинні бути послідовними. Методи токенізації з використанням одних і тих же алгоритмів послаблюють загальну безпеку. Обидва методи мають рішення щодо проєктування та розгортання, які можуть бути задокументовані в криптографічній архітектурі [5; 6].

Наразі відбувається помітна боротьба між постачальниками безпеки за відносні переваги шифрування чи токенізації, які дуже схожі. Незважаючи на публічні заяви деяких постачальників, токенізація насправді еквівалентна формі шифрування. У ході аналізу того, як токенізація чи шифрування можуть використовуватися в умовах підприємства, з'являється розумне правило: якщо потрібно захистити дані, які рідко стають незахищеними, токенізація може бути найкращим підходом, але якщо варто захистити дані, які, можливо, доведеться зняти, щоб дозволити подальшу обробку їх у якийсь момент, найкращим підходом можна вважати шифрування. Бувають випадки, коли кожна технологія перевершує іншу, тому не існує єдиної найкращої технології для всіх застосувань. І лише знання їх переваг дозволяє оптимізувати їх застосування.

Висновки та перспективи подальших досліджень

Питання про доцільність використання шифрування чи токенізації дійсно досі не має однозначної відповіді. У ході вибору інструменту захисту інформації слід враховувати, чи захищені дані від несанкціонованого доступу під час зберігання, передачі та обробки. Інший аспект полягає у тому, чи повинні захищені дані бути унікальними для екземпляра і чи може той самий шифротекст відображати той самий чіткий текст. Крім того, потрібно знати, чи зберігати довжину та формат захищених даних(бо в такому разі для захисту рішення може знадобитися шифрування збереження формату). І, нарешті, потрібно розуміти життєвий цикл даних порівняно з ключовим життєвим циклом.

Зміна криптографічних ключів для шифрування потребує перекладу шифротексту з попереднього ключа на новий ключ, але зміна ключів або таблиць при використанні токенізації також вимагає заміни старих жетонів на новіші лексеми. Основний життєвий цикл управління може мати величезний вплив на програми, що спираються на методи захисту даних.- У різних випадках шифрування і токенізація перевершують одне одного, і лише знання їх переваг та недоліків дозволяє обґрунтувати вибір технологій та оптимізувати їх застосування.

У подальшому, особливої уваги вітчизняних дослідників заслуговують питання правового регулювання механізмів інформаційного захисту, з урахуванням національної безпеки України та інтересів вітчизняних суб'єктів господарювання.

Література

1. Баранов О.А. Інтернет речей (IoT) і блокчейн. "Інформація і право"- № 1(24)/2018 59. с. 59-71.

2. Варавка В. ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СМАРТ-КОНТРАКТІВ. Актуальні проблеми правознавства. 1 (21)/2020. С. 142-151.

3. Гурова А. Кірпачова М. ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ БЛОКЧЕЙНУ В КОСМІЧНІЙ ДІЯЛЬНОСТІ: ОСНОВНІ СФЕРИ ЗАСТОСУВАННЯ. Підприємство, господарство і право. 2020. №11. С. 284-290.

4. Стейплтон, Джефф. Безпека без затемнення: Посібник з конфіденційності, автентифікації та цілісності, преса CRC, публікації Auerbach, ISBN 9781466592148, травень 2014 року.

5. Стейплтон, Джефф. Безпека без затемнення: Посібник з криптографічних архітектур, CRC Press, публікації Auerbach, ISBN 9780815396413, липень 2018 р.

6. Стейплтон, Джефф. «Підробляння модуля апаратної безпеки», журнал ISSA, том 17, випуск 1, січень 2019 року.

7. Мартін, Лютер. «Крипто кут: шифрування проти токенізації», журнал ISSA, том 16, випуск 2, лютий 2018 року.

8. Шифрування у системах обробки інформації. Вікіпедія. URL : https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F

9. ANSI X9.8: 2015 (ISO 9564: 2011) «Фінансові послуги: управління та безпека персонального ідентифікаційного номера (PIN) - Частина 1: Основні принципи та вимоги до ПІН-кодів у карткових системах».

10. ISO / IEC 18033: 2015 «Інформаційні технології: методи безпеки – алгоритми шифрування - частина 1: Загальні».

11. Юридична енциклопедія: В 6 т. / Редкол.: Ю70 Ю. С. Шемшученко (голова редкол.) та ін. — К.: «Укр. енцикл.», 1998. ISBN 966-7492-00-1

12. ANSI X9. 119: 2017 «Фінансові послуги для роздрібної торгівлі: вимоги щодо захисту даних чутливих платіжних карток - Частина 2: Впровадження системи післякеризації токенізації. Стандарт (FIPS) 197 «Розширений стандарт шифрування (AES)», листопад 2006р.

13. Facebook Messenger isaddingend-to-endencryptionforvoiceandvideocalls. ByAdiRobertson. TheVerge. Aug 13, 2021. URL : https://www.theverge.com/2021/8/13/22623627/facebook-messenger-video-calls-end-to-end-encryption

14. АлександрОгнев. Skillbox: Образовательная платформа. URL : https://skillbox.ru/course/cybersecurity/

15. ФБР самостійно зламало iPhone стрілка з Сан-Бернардіно. 29 березня 2016. BBC News. URL : https://www.bbc.com/ukrainian/science/2016/03/160329_apple_fbi_iphone_vs

16. Policecanaccesssuspects' FacebookandWhatsAppmessagesindealwith US. TheSundaytimes. SaturdaySeptember 28 2019, URL : https://www.thetimes.co.uk/article/police-can-access-suspects-facebook-and-whatsapp-messages-in-deal-with-us-q7lrfmchz?wgu=270525_54264_15696934907908_9d4966d9ec&wgexpiry=1577469490&utm_source=planit&utm_medium=affiliate&utm_content=22278&region=global

17. DOJ issuesnewwarningtobigtech: Dataandprivacycouldbecompetitionconcerns. ByTonyRomm. November 8, 2019 TheWashingtonPost. URL : https://www.washingtonpost.com/technology/2019/11/08/doj-issues-latest-warning-big-tech-data-privacy-could-be-competition-concerns/

18. Facebook'spushforend-to-endencryptionisgoodnewsforuserprivacy, aswellasterroristsandpaedophiles. TheConversation. December 16, 2019. URL : https://theconversation.com/facebooks-push-for-end-to-end-encryption-is-good-news-for-user-privacy-as-well-as-terrorists-and-paedophiles-128782

19. Exclusive: MessagingappTelegrammovestoprotectidentityofHongKongprotesters. REUTERS. AUGUST 31, 2019 URL : https://www.reuters.com/article/us-hongkong-telegram-exclusive-idINKCN1VK2NI

20. МессенджерBriar на основеТогвышелизстадии бета. ГЕОРГИЙ

ЛЯМИН | 11 МАЯ 2018. URL : https://www.iguides.ru/blogs/appdt/messenger-briar-on-the-basis-of-tor-is-out-of-beta/

21. Стандарт захисту даних платіжних карток (PCI) «Вимоги та процедури оцінки безпеки v3.2», квітень 2016 р. URL : https://ru.pcisecuritystandards.org/_onelink_/pcisecurity/en2ru/minisite/en/docs/PCI_DSS_v3_2_RU-RU_Final.pdf

22. Промисловість платіжних карток (PCI) «Настанови щодо безпеки продукту для токенізації v1.0», квітень 2015 р.

23. «Стандарт захисту даних платіжних карток» (PCI) «Настанови щодо токенізації v2.0», серпень 2011 р.

24. TheDifferenceBetweenFormat-PreservingEncryptionandTokenization. URL: https://www.comforte.com/fileadmin/Collateral/comforte_FS_tokenization_vs_FPE_WEB.pdf

SUMMARY

The article considers the similarities and differences between two popular cryptographic methods of information transfer: encryption and tokenization. It is emphasized that when deciding on the choice of protection methods, a number of factors should be taken into account, including the way the data is used and the key management life cycle of the organization.

In the process of research, the author gives different approaches to the definition of "encryption", "cipher", highlighting their common component. As the main feature of encryption, it is proposed to consider the use of cryptographic keys to convert data (clear information) from readable to unreadable (ciphertext) form. In this case, "decryption" is reverse encryption, the use of cryptographic keys to convert encrypted text back into its original "transparent and clear" form.

In the process of analyzing the approaches to the definition of "tokenization", the author singles out, as a common feature, that the main description of tokenization is the use of cryptographic method to replace readable transparent text with other readable transparent text.

Particular attention is paid to the review of attempts by state security agencies of different countries to control the studied methods of information protection, or to counteract them. The author mentions the confrontation between the US government and Apple and Facebook, the use of the Hong Kong government features of the Telegram application. At the same time, the author in no way provides an assessment of the ethics and legitimacy of government interference in the work of corporations and their products, focusing exclusively on the technical features of a mechanism for protecting information.

Among other things, the differences between symmetric and asymmetric encryption, tabular and random tokenization methods are given.

Keywords: information, information security, legal regulation, blockchain, cipher, encryption, decryption, tokenization, detokenization.