УДК 004.56.5:003.26 **СЕКЦІЯ 7**

ДОРЕНСЬКИЙ О. П, ІСАЧЕНКОВ Е. В.

СТРУКТУРНО-ФУНКЦІОНАЛЬНА МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КЛІЄНТСЬКОГО ЗАСТОСУНКУ БАЗИ АНАЛІТИЧНИХ ДАНИХ ҐРУНТІВ

This research addresses the issue of ensuring cybersecurity and protecting the information of a soil analytical information cloud database. This database is a component of the information system for soil bonitation that is implemented within the IT project. It consists of the Dropbox cloud service and a client application. The Dropbox technology provides a sufficient level of data cybersecurity, while the protection of the client application's information is still a relevant task.
Therefore, the goal of the research is to synthesize a structural-functional model of the cloud database client. Methods used include structural-genetic analysis, synthesis, modeling, as well as Dropbox technology and the "Kalyna" encryption algorithm (DSTU 7624:2014). The result of the research is a structural-functional model for ensuring the cybersecurity of the client service of the soil analytical information database. The application of this model will enable the practical implementation of data cybersecurity in the soil bonitation information system. This is achieved through the cryptographic protection of information using the "Kalyna" symmetric block cipher algorithm. Thus, the data that is created, transmitted, and processed within the information system (cloud server, client application) is protected.

Ключові слова: *захист інформації, кібербезпека, шифр Калина, база даних, Dropbox API.*

Реалізація ІТ-проєкту з цифрової трансформації бонітування ґрунту передбачає забезпечення кібербезпеки і захисту даних, які обробляються в інформаційній системі. За результатами аналізу технологій зберігання даних [1-4] обрано хмарний сервіс Dropbox API. Ця технологія має декілька напрямків реалізації, передача даних відбувається за протоколом HTTPS, до якого входить захищений протокол TLS з асиметричним шифруванням, тому безпека передачі даних забезпечена. Також є захищеним доступ Access Token, який відповідає за авторизацію клієнта до хмарного середовища. Ці фактори свідчать про достатній рівень захищеності передачі інформації до хмари, тобто Dropbox забезпечує належний рівень серверного кіберзахисту. Разом з тим, актуальною є задача кібербезпеки й захисту інформації клієнтського застосунку бази даних, тому метою цієї праці є синтез структурно-функціональної моделі клієнта бази аналітичних даних ґрунту.

У клієнтському застосунку дані передаються файловим потоком, тож є небезпека витоку, модифікації. Для шифрування даних пропонується застосовувати алгоритм симетричного блокового перетворення [5], перевагами якого є висока швидкодія програмної реалізації на сучасних платформах, високий рівень стійкості та наявність різних режимів роботи. Шифр використовує унікальний ключ для шифрування та дешифрування.

"Калина" є блочним симетричним шифром, тож дані шифруються та дешифруються у фіксованих блоках 128 біт або 16 байт. Пропонується до реалізації режим CBC, при якому над кожним блоком виконується XOR з попереднім зашифрованим блоком для уникнення шаблонів у вихідних даних. Перший блок XOR-иться з ініціалізаційним вектором (IV), згенерованим випадково; це забезпечує ще один рівень захисту передачі даних.

Вхідна інформація для шифрування/дешифрування ділиться на блоки по 128 біт. Оскільки останній блок малоймовірно буде рівним 128 біт, тож для шифрування слід використати функцію додавання: доповнення в останньому блоці бітів, яких бракує. При дешифруванні навпаки: в останньому блоці біти додані видаляються; тому підлягає реалізації функція видалення.

Структурно-функціональна модель забезпечення кібербезпеки клієнтського сервісу бази аналітичних даних ґрунтів представлена на рис. 1. До її складу входять функціональні елементи бази даних, файлів для шифрування і дешифрування, генератора ключів та процесів алгоритму "Калина": запису й зчитування блоків даних, ділення, віднімання, додавання біт інформації та процесора безпосередньо симетричного блокового перетворення.

© ДОРЕНСЬКИЙ О.П, ІСАЧЕНКОВ Е. В. 2024

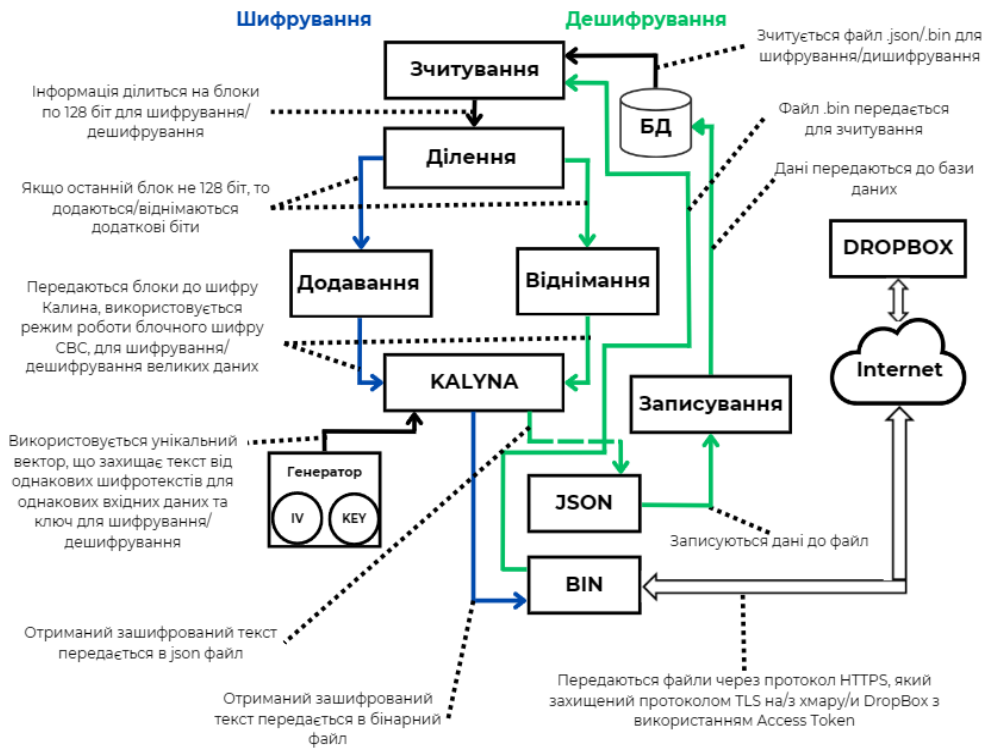

Рис. 1 Модель забезпечення кібербезпеки клієнтського застосунку бази аналітичних даних ґрунтів

Застосування запропонованої моделі під час реалізації ІТ-проєкту цифровізації бонітування ґрунту дозволяє практично реалізувати забезпечення кібербезпеки й захисту інформації клієнтського застосунку хмарної бази даних. Шифрування інформації, яка обробляється у інформаційній системі, за допомогою симетричного шифру “Калина” в режимі CBC гарантує конфіденційність даних у разі витоку з серверної або клієнтської частини ІС.

СПИСОК ЛІТЕРАТУРИ

1. Google Drive API. URL: https://developers.google.com/drive/api/reference/rest/v3 (дата звернення: 21.10.2024).
2. Amazon S3: Introduction. URL: https://docs.aws.amazon.com/AmazonS3/ latest/userguide/GetStartedWithS3.html (дата звернення: 21.10.2024).
3. Azure Storage Blobs: Introduction UR: https://learn.microsoft.com/en-us/ azure/storage/blobs/storage-blobs-introduction (дата звернення: 21.10.2024).
4. Dropbox Fundamentals Course. URL https://learn.dropbox.com/self-guided-learning/ dropbox-fundamentals-course/how-to-use-dropbox (дата звернення: 21.10.2024).
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Введ. 01-07-2015]. Вид. офіц. Київ: Мінекономрозвитку України, 2016. 228 с.

ДОРЕНСЬКИЙ Олександр Павлович – к. т. н., доцент; доцент кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет, просп. Університетський, 8, м. Кропивницький, Україна, 25006; e-mail: dorenskyiop@kntu.kr.ua; ORCID: 0000-0002-7625-9022.

Наукові інтереси: *технології проектування й тестування складних програмних систем.*

ІСАЧЕНКОВ Едуард Віталійович – здобувач вищої освіти за спеціальністю “Кібербезпека та захист інформації”; Центральноукраїнський національний технічний університет, просп. Університетський, 8, м. Кропивницький, Україна, 25006; e-mail: isachenkov.eduard26@gmail.com.

Наукові інтереси: *кібербезпека та захист інформації інформаційних систем.*