Реалізація проекту платформи була поділена на дві частини – створення серверної (бекенд) та клієнтської (фронтенд) частини. Серверна частина - REST API система, побудована на мікросервісній архітектурі та розгорнута з використанням технологій контейнеризації, завдання якої приймати запити по HTTP протоколу від клієнта (веб-додатку), обробляти їх та повертати дані в JSON форматі.

У даному проекті функціонують п’ять мікросервісів (рис.1):

- Api Gateway – розподільник та агрегатор запитів, надає лише дозволений функціонал для користувачів з різними рівнями доступу, та збирає дані з кількох мікросервісів у разі потреби.
- Identity Service служить для авторизації, реєстрації та зберігання персональних даних користувачів.
- Members Service служить для зберігання та обробки даних про студентів, викладачів, груп та відгуків.
- Education Service служить для зберігання та обробки усього, що торкається навчального процесу – домашні завдання, розклад, відмітки, оцінки, екзамени.
- File Service служить для роботи з зовнішніми додатками для роботи з файлами та зображеннями. Для зберігання та скачування файлів (домашніх завдань) використовується Amazon S3.

Кожен з цих мікросервісів частково або повністю може функціонувати без інших.

У цьому проекті кожен із мікросервісів був розгорнутий у окремому контейнері за допомогою технології Docker.

УДК 004.77

Студентка групи 5 дТН Ю.В. Калашнікова
Г.В. Головко, к.т.н.,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

КРИПТОЛОГІЧНІ АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ

Криптографі́чний за́хист інформа́ції – різновид захисту інформації з обмеженим доступом, розголошення якої завдає (або може завдати) шкоди державі, суспільству чи особі. КЗІ реалізують шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Проблеми безпеки інформації за останні роки набули виключної актуальності, при цьому забезпечення захисту інформаційних технологій приймає комплексний характер. Серед різних методів захисту інформації (технічних, правових, організаційних та

інших) найважливіше місце займають криптографічні методи. За останні два десятиріччя криптологія сформувалася у самостійну наукову дисципліну, що має свою специфіку постановок задач та методів їхнього дослідження. Знання основних понять криптології, володіння криптографічними методами захисту інформації за сучасних умов вкрай необхідні будь-якому фахівцю, що займається створенням систем захисту інформації.

До засобів КЗІ належать апаратні, програмні та апаратно-програмні системи і комплекси, що реалізують криптографічні алгоритми перетворення інформації; захищають від нав'язування неправдивої інформації, включаючи засоби імітозахисту та електронного підпису; призначені для виготовлення та розподілу ключових документів, які використовують у засобах КЗІ, незалежно від виду носія ключі інформації; входять до систем та комплексів захисту інформації від несанкціонованого доступу.

Методи криптографії поділяють на дві групи – підставлення (заміни) і переставлення. Підставлення метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза – ключ. У загальному випадку у криптографії ключ – це послідовність бітів, що використовуються для шифрування та розшифрування даних.

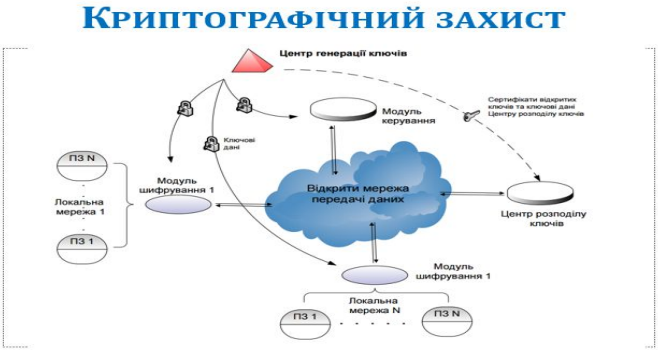
Подібний шифр дуже швидко можна розкрити, вивчивши повторюваність символів та короткі слова «і», «або», «за» і т. ін. У разі використання перестановки алгоритму змінюються не символи, а порядок їх розміщення в повідомленні.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення електронних (цифрових) підписів (ЦП) – сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала.

Залежно від доступності ключів розрізняють:

- симетричне шифрування – для шифрування і розшифрування використовується один ключ. Такі системи із закритим ключем реалізовані, наприклад, в архіваторах даних. Це зручно для шифрування приватної інформації, але під час передавання повідомлення по каналах зв'язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування. У принципі, якщо можна таємно передати ключ, то можна передати і таємну інформацію, тоді відпадає необхідність у шифруванні, а якщо такої можливості немає, шифрування даремне;
- асиметричне – для шифрування використовується один, відкритий (публічний, загальнодоступний) ключ, а для дешифрування – інший, закритий (секретний, приватний). Це робить непотрібним таємне передавання ключів між кореспондентами. Відкритий ключ марний для

дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи – ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати. Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA, названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.



Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює необхідні передумови для заміни паперового документообігу електронним і переходу до здійснення електронних операцій. [1]

Література

1. https://sites.google.com/site/zahistlokalnoiemerezi/zahist/kriptograficnij-zahist.

УДК 621.391

Ю.М. Здоренко, к.т.н.,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»,
М.С. Здоренко

СИСТЕМА ВИЯВЛЕННЯ МОДИФІКОВАНИХ АТАК В ІНФОРМАЦІЙНО- ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Пріоритетним напрямком кібернетичного захисту сучасних інформаційно-телекомунікаційних мереж (ІТМ) критичної інфраструктури є використання систем виявлення атак. Аналіз даних про характеристики трафіку такими системами дозволяє здійснювати класифікацію можливої атаки та здійснити заходи щодо її попередження. Поява невідомих або модифікованих атак обмежує та робить неефективним використання систем виявлення на основі сигнатурних методів. Аномальний характер