коду, користувач повинен підтвердити операцію, обравши банківську картку, якою він хоче оплатити рахунок, та натиснути кнопку “Підтвердити” (див.рис. 3).

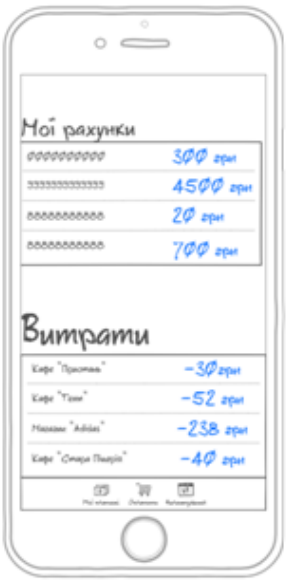

Рисунок 2 – Прототип головного вікна додатку

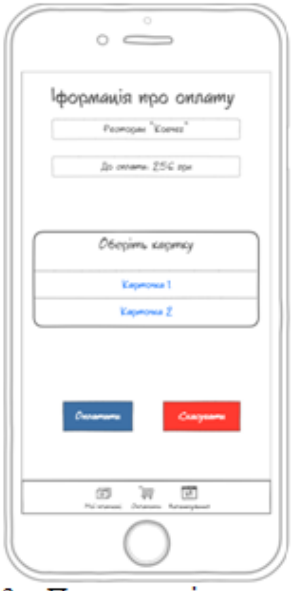

Рисунок 3 – Прототип вікна додатку для проведення операції оплати

Висновок

У роботі розглянуто спосіб безконтактної оплати послуг, використовуючи тільки мобільний телефон, який оснований на використанні технології SWIFT з допомогою бібліотеки “QuuR-swift” для генерування QR кодів. Даний принцип роботи додатку дозволяє зекономити час, а також вносить зручність в безконтактну оплату послуг.

Список використаних джерел

1. Сайт документації SWIFT [Електронний ресурс]. Режим доступу - https://developer.apple.com/documentation/swift
2. Документація бібліотеки QuuR-swift [Електронний ресурс]. Режим доступу - https://github.com/cam-inc/quur-swift
3. Документація API Приват банку [Електронний ресурс]. Режим доступу - https://api.privatbank.ua/

УДК 004.056:681.51

МОДЕЛЬ ЖИВУЧОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧОЇ СИСТЕМИ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Літава Г.В.[1)],Якименко І.З.[2)], Філіпович М.В.[3)], Мачуляк М.В.[4)]

[1)] *Університет у Бєльско-Бяла, Республіка Польща, к.т.н*

Тернопільський національний економічний університет

[2)] *к.т.н;* [3)] *магістрант;* [4)] *студент*

І. Постановка проблеми

Функціональна безпека сучасних інформаційних технологій ґрунтується на дослідженнях живучості інформаційно-управляючих систем (ІУС), які належать до одного з провідних наукових напрямів найбільших інженерних викликів XXI століття, які визначив науковий фонд NSF. Крім того, необхідно виділити окремий клас ІУС, що ґрунтуються на використанні математичного апарату еліптичних кривих (ІУСЕК), тобто ІУС, в пристроях яких закладені базові операції на ЕК [1], в тому числі Elliptic Curve Cryptography Device (ECCD або криптографічні пристрої на еліптичних кривих –

КПЕК). Тому, актуальною науковою задачею є вдосконалення, опрацювання і впровадження моделей і технічних засобів оптимізації живучості ІУСЕК.

На сьогоднішній день постає питання шифрування та розшифрування в реальному часі на криптографічних пристроях та оцінювання,підвищення живучості ІУСЕК. Слід відмітити, що основною задачею забезпеки КЕК є забезпечення стійкості алгоритму шифрування[2], яка ґрунтується на складно обчислювальній проблемі дискретного логарифмування[3].Вдосконалення методів виконання базових операції в знаходженні цього логарифму призводить до зменшення часових характеристик.

II. Мета роботи

Основною метою даної роботи є розробка моделі живучості інформаційно-управляючих систем на основі використання математичного апарату ЕК, яка дозволила б оптимізувати часові характеристики за рахунок використання теоретико-числового базису Крестенсона[4,5].

III. Моделі та живучість

В працях [6, 7] запропоновані відмовостійкі багатопроцесорні ІУС, які покладені в основі оцінки стану ІУСЕК, тобто через P позначимо продуктивність системи, яка базується на апаратних засобах криптографічних операцій на ЕК. Крім того введемо основні складові ІУСЕК:

p_{wwf}– імовірність безвідмовної роботи ІУСЕК;

f_s– функція живучості, тобто мінімальна підмножина функцій ІУСЕК з найвищим пріоритетом, виконання яких необхідно для того, щоб система не перейшла до небезпечного стану;

P_s– продуктивність ІУСЕК, необхідна для виконання функцій живучості та нижче за яку виникає аварія;

m – загальна кількість функцій живучості;

p_{ds}– ймовірність переходу ІУСЕК на часовому інтервалі t до небезпечного стану;

n – загальна кількість процесорних пристроїв в ІУСЕК;

n_{ECCD}– кількість пристроїв ECCD у системі, що виконують криптографічні операції на еліптичних кривих;

x – вектор стану ІУСЕК;

X_{ds}– множина, яка відповідає небезпечним станам ІУСЕК;

x_i та x_j – компоненти вектора x, які відповідають стану i-го процесорного пристрою та j-го ECCD ($x_i = x_j = 0$ – для відмови; $x_i = x_j = 1$– для працездатності);

P_i та P_j– продуктивність i-го процесорного пристрою та j-го ECCD;

P_x – продуктивність ІУСЕК в стані, що відповідає вектору x.

З врахуванням перелічених складових отримується удосконалена модель живучості ІУСЕК, яка записується з допомогою рівнянь:

$$P_x = \sum_{i=1}^{n-n_{ECCD}} \alpha_i \, P_i + \sum_{j=1}^{n_{ECCD}} \alpha_j \, P_j \,, \tag{1}$$

$$p_{ds}(t) = \sum_{x \in X_{ds}} p_x(t)\Big|_{\forall x \in X_{ds}} \,, \tag{2}$$

де

$$p_x(t)\Big|_{\forall x \in X_{ds}} = \prod_{i=1}^{n} p_i^{x_i} \left(1 - p_i\right)^{1-x_i} - \prod_{j=1}^{n-n_{ECCD}} p_j^{x_j} \left(1 - p_j\right)^{1-x_j} \,, \tag{3}$$

причому $p_{wwf} = p\left(P_x \geq P_s\right)$, $P_s = \sum_{f=1}^{m} P_{s.f}$.

Наведені рівняння дозволяють знайти імовірність переходу ІУСЕК в часовому інтервалі t до небезпечного стану, викликаного зниженням її продуктивності внаслідок відмов ECCD.

Основна особливість моделі полягає в заміні операції модулярного множення цілих багаторозрядних чисел додаванням за модулем, яке проводиться на основі використання теоретико-числового базису Крестенсона, а також застосуванням паралельного додавання чисел, дає змогу прискорити виконання операції на відміну від традиційного підходу. Паралельне сумування полягає на поділі цих чисел великої розрядності на слова, розмір яких дозволить безпосередньо виконати операцію додавання за допомогою вбудованих в процесори суматорів з використанням стандартних типів даних. Зазвичай в математичних операціях на еліптичних кривих виконується додавання точок

або їх подвоєння. В такого типу операціях застосовуютьсядії над числами, такі як сумування по модулютамодулярне множення багаторозрядних чисел.

IV. Висновки

В роботі представлена модель живучості ІУСЕК, основна особливість якої полягає в заміні операції модулярного множення цілих багаторозрядних чисел додаванням за модулем на основі використання теоретико-числового базису Крестенсона, а також застосуванням паралельного додавання чисел, дає змогу прискорити виконання операції на відміну від традиційного підходу.

Список використаних джерел

1. Якименко І.З.Теоретичні основи зменшення часової та апаратної складності систем захисту інформаційних потоків на основі еліптичних кривих з використанням теоретико-числового базису Радемахера-Крестенсона. /І.З. Якименко, М.М. Касянчук, В.В. КімакВісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». – №694.– 2012. – с. 118–126.
2. Yakymenko I.Z. Reliability of Schoof algorithm and its computational complexity// I.Z. Yakymenko, Y.I.Kinakh./Proceedings of the Xth International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics". – Lviv-Polyana. – 2009. – С. 107.
2. Карпінський М.П.Підвищення ефективності обчислення точок на еліптичних кривих над обмеженими полями/М.П. Карпінський, І.З. Якименко, А.О. Ботюк //Вісник Тернопільського державного технічного університету імені Ів.Пулюя, - Том 8, - №4 – 2003. – С: 67 – 73.
3. Касянчук М.М.Теоретичні основи виконання медулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера/ М.М. Касянчук, Я.М.Николайчук І.З.Якименко, Т.М.Долинюк.//Інформатика та математичні методи в моделюванні. – №2. – 2011. – С. 123–130.
4. НиколайчукЯ.М. Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона/ Я.М.Николайчук, М.М.Касянчук, І.З. Якименко, С.В.Івасьєв// Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». – №806.– 2014. – с. 195-199
5. Мораведж Сейед Милад. Оптимизация некоторых параметров реконфигурируемых отказоустойчивых многопроцессорных систем / Гроль В.В., Мораведж Сейед Милад, Шурыга А.В.// Інформаційно-керуючі системи на залізничному транспорті. Тези доповідей.- 2010.- №4(додаток).- С. 7.
6. Мораведж Милад. О взаимном тестировании компонентов в многопроцессорных системах / Гроль В.В., Романкевич В.А., Мораведж Милад, Потапова Е.Р.// Радіоелектронні і комп'ютерні системи.- 2012.- №7.- С.131-134.

УДК 58.009

МОБІЛЬНЕ НАВЧАЛЬНЕ СЕРЕДОВИЩЕ ДЛЯ МОДЕЛЮВАННЯ БУДОВИ РОСЛИННИХ ОРГАНІЗМІВ

Ліхота О.І.

Тернопільський національний економічний університет, магістрант

І. Постановка проблеми

Навчальна програма з біології в Україні на сьогоднішній день являє собою відсталий, неефективний та нетехнологічний напрям. Для виправлення ситуації потрібне впровадження нових технологій та засобів, лише за таких умов можна сподіватись, що в майбутньому будуть добре підготовлені освідченні спеціалісти. ІТ-технології заповнюють усі галузі, цьому важко суперечити, попри те, навчання у школах не рідко залишається на етапі «СРСР».

Всі ми знаємо, щоб досягнути успіху у певній галузі потрібно багато працювати, краще за все почати з дитинства, за таких умов у людини буде значно більше часу для розвитку.

Рослини просто незамінні, бо надають нам повітря, щоб дихати, ягоди, щоб їсти, сік, щоб втамувати спрагу, важко заперечувати нашу потребу в них.

Рослинний світ неймовірно цікавий та важливий для вивчення, а ІТ-технології надають можливість передавати інформацію швидко, якісно та чітко.

Смартфон чи планшет є невід'ємною частиною кожного з нас, він приходить до нас на допомогу при кожній потребі, дивно, що ці зручні винаходи не використовуються у навчальній програмі у корисних цілях.