|  |  |  |  |
| --- | --- | --- | --- |
| МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Тараса Шевченка ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ  **Кафедра програмних систем і технологій**  Дисципліна  **«АНАЛІЗ ВИМОГ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»**  **Лабораторна робота № 1**  **«АНАЛІЗ ТА ВСТАНОВЛЕННЯ ВИМОГ»**  **на тему:**  **«Автоматизована система безготівкових електронних платежів»** | | | |
| **Виконав:** | Гоша Д.О | **Перевірив**: | Юрчук І. А. |
| Група | ІПЗ-23 | Дата перевірки |  |
| Форма навчання | Денна | Бали |  |
| Спеціальність | 121 |
| 2021 | | | |

**Мета**: створити попередній опис проблеми у деякій предметній галузі та проаналізувати існуючі програмні продукти, які в ній функціонують.

# Завдання:

1. Вибрати предметну область із запропонованого переліку або власну узгоджену з викладачем (Додаток 1).
2. Зробити опис обраної предметної галузі
3. Зробити опис проблеми, яка підлягає вирішенню.
4. Здійснити пошук в мережі Інтернет п’яти існуючих програм-аналогів (сайтів) для обраної предметної області (вітчизняні та закордонні ресурси).
5. Описати кожну із розглянутих програмних систем за наступним планом:
   * назва продукту, компанія-виробник;
   * основні функціональні можливості;
   * переваги програмної системи;
   * недоліки програмної системи.
6. Здійснити порівняння існуючих програм-аналогів і внести дані в таблицю.
7. На основі проведеного аналізу скласти перелік вимог до програмної системи для заданої предметної області.

# Виконання завдання:

1. Автоматизована система безготівкових електронних платежів.
2. Програмне забезпечення, що створене задля : створення , отримання , обміну цифровими активами серед учасниками мережі без участі адміністрації сайту.
3. Достатньо суттєва проблема це безпека засобу збереження грошей. Тому система має бути крайнє надійною та захищеною від (exploit’s) через запобігання (0 spend) – витрата грошей з чужих гаманців, або ж захист від дампу приватного ключа , що слугує основним медіатором доступу до грошей у мережі. Тобто основна ідея проекту – створення зручного та надійного ПЗ з зрозумілим інтерфейсом для зберігання ключа, автоматизації переказів , підрахунок поточної пріорітетної комісії та зміна номеру приватного гаманця для отримання коштів так званий (dynamic wallet).
4. **Програми аналоги:**
   * Electrum,
   * Trezor Hardware Wallet,
   * Exodus,
   * Blockchain,
   * Coinbase
   * Metamask
5. **Короткий опис програм - аналогів**
   * **Electrum** є простим та зручним гаманцем для зберігання Біткоїна. Він був розроблений у листопаді 2011. Це робить його одним з найстаріших Біткоїн гаманців у світі. До речі, на думку багатьох (погляньте на Electrum відгуки) це ще й найкращий Біткоїн гаманець.  
     Переваги: Один з найстаріших гаманців для Біткоїна, дуже простий у використанні, програмний, інформація не зберігається на серверах, відкритий вихідний код, використовує двофакторну автентифікацію.  
     Недоліки: Мав проблеми з безпекою, підтримує тільки Біткоїн.
   * **Trezor** був першим випущеним апаратним гаманцем для криптовалюти. Це апаратний гаманець, який дозволяє безпечно зберігати, відправляти та отримувати багато різних криптовалют. Гаманець був уперше випущений у 2014 році компанією SatoshiLabs, яка знаходиться у Чеській Республіці.  
     Переваги: Першокласна безпека, дуже відомий гаманець, зберігає величезну кількість криптовалют ,постійні оновлення.  
     Недоліки: Дорогий, мав проблеми з несанкціонованим доступом.
   * **Exodus Wallet** є відносно новим програмним гаманцем, але вже встиг завоювати певну популярність. Його творцями стали Дж.П. Річардсон і Деніел Кастагнолі. Річардсон раніше займався написанням коду для безлічі криптовалютних проектів, а Кастагнолі працював дизайнером у таких великих компаніях як Apple, BMW і Nike.  
     Переваги: Простий у використанні, має підтримку клієнтів, великий вибір криптовалют, програмний гаманець, вбудована функція обміну, автоматичне налаштування комісії.  
     Недоліки: Вразливий до проблем безпеки ,комісія може бути досить високою.
   * **Blockchain** (компанія) з'явилася на світ ще далекого 2011 року. Це базується в Люксембурзі підприємство, яке спеціалізується на різних сферах технології блокчейну – компанія надає дані та статистику про Біткоін, різні метрики, гаманець криптовалют (у центрі нашої уваги на сьогодні) та послуги з так званої розвідки блокчейну.  
     Переваги: Низька комісія за транзакції, вбудовані функції біржі, дуже захищений, найпопулярніший гаманець у світі.  
     Недоліки: Низька анонімність, централізованість, ваші приватні ключі зберігаються на їхніх серверах
   * **Coinbase** є брокер-обмінником, де ви можете купувати та торгувати Біткоіном, а також іншими криптовалютами. Вона відрізняється від традиційних криптовалютних бірж та обмінників, оскільки дозволяє купувати крипто за допомогою фіатних грошей.  
     Переваги: Простий у використанні інтерфейс, пропонує лише 4 надійні криптовалюти: BTC, LTC, ETH та BCH, приймає транзакції у фіатній валюті, кілька способів оплати. регулюючі норми, що роблять платформу безпечною та легітимною, дотримується політики щодо збереження прозорості та надійності;  
     Недоліки: Доступна не в усіх країнах, oбмежує те, скільки ви можете витратити або зняти, комісія вище середнього, суворі правила KYC дозволяють відстежувати дії користувачів, що перешкоджає анонімності (багато Coinbase відгуки присвячені саме цій проблемі), суворе дотримання всіх податкових процедур, які змушують ділитися вашими даними з податковими органами.
   * **Metamask** – це криптовалютний гаманець, який можна використовувати у браузерах Chrome, Firefox та Brave. Він виглядає як розширення для браузера. Він налагоджує взаємодію між звичайними браузерами та блокчейном Ethereum.  
     Переваги: Відкритий вихідний код, налаштування HD, вбудована покупка монет, простий інтерфейс, підтримка клієнтів, локальне сховище ключів.  
     Недоліки: Доступ через браузер , онлайн.
6. **Таблиця порівняннь аналогів**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Electrum** | **Trezor** | **Exodus Wallet** | **Blockchain** | **Coinbase** | **Metamask** |
| Повністю відкритий вихідний код | Так | Так | Ні | Так | Ні | Так |
| Гаманець – це API, SPV чи Node? | API | API | API | API | API | API |
| Резервне копіювання примусово? | Так | Так | Ні | Ні | Ні | Так |
| Інтеграція з апаратним гаманцем? | Так | Так | Так | Так | Ні | Так |
| Bech32 | Так | Так | Так | Так | Ні | Так |
| Чи може бути багато гаманців одночасно? | Ні | Так | Ні | Так | Ні | Ні |
| Фіатний обмін | Ні | Так | Ні | Так | Так | Так |
| Чи існують ключі на серверах сервісів? | Ні | Ні | Ні | Ні | Так | Так |
| Правова політика | Ні | Так | Так | Так | Так | Так |
| Тільки біткойн? | Так | Ні | Ні | Ні | Ні | Ні |
| Тип (Онлайн , програмний чи апаратний) | Програмний | Апаратний | Програмний | Онлайн | Онлайн | Онлайн |
| Чи можете бути заблоковані? | Ні | Ні | Ні | Так | Так | Так |
| Настроюваний інтерфейс користувача (Інтерфейс користувача) | Так | Ні | Так | Так | Ні | Ні |
| PSBT (частково підписані біткойн-транзакції) | Так | Ні | Ні | Ні | Так | Так |
| Вибір комісії | Так | Так | Так | Не повний | Ні | Не повний |

1. **Опис вимог на основі проведеного аналізу**

Сучасні тенденції прямують до децентралізації та зменьшення регулювання та контролю криптовалют , тому що саме для вільних безготівкових платежів , які не облягають оподаткуванням, вони і створювались. Перш за все користувачі спрямовуюсь увагу на централізацію , безпеку і анонімність. Дуже важливо тримати баланс між законним обігом валют та конфеденційністю користувачів продукту.

Що до безпеки – програмне забезпечення має бути добре протестовано та перевірено на можливі вразливості на інжекти. Взято за уваги помилки попередніх продуктів та передчасне виправлення.

З приводу анонімності та централізації. Безумовно я проти KYC, та зберігання та обробки буль яких приватних даних користувачів. Це сприятиме на деяким ураженя функціоналу . А саме фіатна купівля та біржевий обмін. Але, на мою думку, це навпаки заохотить користувачів.

Слід пам’ятати про зручний та гнучкий інтерфейс. З усіх прикладів , що ми розглянули , найзручніший у *Exodus Wallet* . Проте ним займався дизайнер Apple, BMW і Nike , ми маємо взяти це до уваги і спробувати зробити краще. Зручний інтерфейс заохочує користувачів , особливо коли він функціональний та інтуїтивно зрозумілий.

Із типів (Онлайн , програмний чи апаратний) , я вирішив вибрати – програмний з можливістю інтеграції апаратних гаманців. Чому саме програмний? Тому що він представляю деяку медіану зручності (можна використовувати повсякденно), на відміну від апаратного. Та захищеність , що не дозволяє розробити онлайн тип. До того ж він доволі простий у розробці , не вимагає складностей у обслуговувані. Ми не зберігаємо приватні ключу , тому навіть якщо наша система дати збій або буде скомпрометована, порушники не отримають приватні ключі та доступи до гаманців користувачів. Однак це несе інші проблеми пов’язані з безпекою. Тепер кожному користувачу доведеться піклуватись про свою безпеку самостійно. Тим самим наш продукт буде не дуже задовольняти потреби новачків або людей , що не піклуються власною безпекою.

# Висновок:

Отримано аналіз програмних застосунків конкурентів. Створивши таблицю порівняли їх плюси та мінуси , визначили необхідні функіональні вимоги. Вимоги до конфеденційності та безпеки. Визначили можливі проблеми та вразливості ринку для вирішення та привести нововедення у ринок IT послуг. Також отпримаємо деякий список вимог до розробки , та можливо уникнимо допрацювання ПЗ, виконавши повне ТЗ одразу.