3. User Story – короткий опис функції продукту з погляду користувача. Стандартна формула User Story виглядає так: Як (тип користувача) + я хочу (дія / ціль) + щоб (результат).

4. Jobs to be Done (JTBD) – це фреймворк, який розповідає про потреби користувача з погляду найму продукту на роботу. Якщо User Story працює з уже відомою та зрозумілою аудиторією, то JTBD спрямований на те, щоб залучати нових користувачів, створювати інновації та виходити за межі. Базова формула JTBD виглядає так: Коли (опис ситуації) + я хочу (мотивація) + щоб (результат).

5. Service Blueprint – це фреймворк, який поєднує CJM і Business Process Model and Notation (BPMN). Насправді це карта шляху користувача лише з боку внутрішніх процесів компанії [5].

Висновки. Проєкт можна порівняти з будинком. Напевно, важко побудувати будинок без фундаменту. У випадку створення чи покращення послуги фундамент – це чіткі й структуризовані знання про продукт і цільову аудиторію. Можна інвестувати чималі кошти в проєкт, найняти найкращих працівників із різних галузей, але без якісної аналітики бізнес не принесе задоволення ані вам, ані користувачеві.

Головна мета загальнодоступності і зручності використання – зрозуміти, наскільки просто людям користуватися продуктом. Отже, спираючись на відгуки користувачів, розробникам буде простіше зорієнтуватись, які коригування та додавання потрібно буде застосовувати до дизайну у майбутньому.

Abstract. The article is devoted to the review of UX research methods in the creation of IT products. The work describes what product IT is, the stages of creating IT products. Emphasis is placed on UX research methods. UX research is very useful for developing a product strategy and algorithmizing solutions that would meet the needs of users. Companies are thinking more and more about improving the user experience because it really helps.

Keywords: IT, product IT, IT industry, UX research.

СПИСОК ЛІТЕРАТУРИ

1. Що таке IT? URL: https://inneti.com.ua/it/it-produkty/detalnishe-pro-it/pro-it/
2. «Управління IT проектами»: конспект лекцій / Тернопільський національний економічний університет. Тернопіль. 2013. 44 с. URL: http://dspace.wunu.edu.ua/retrieve/19638/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%97.pdf.
3. Зелінська О. В., Потапова Н. А., Волонтир Л. О., Інформаційні системи та технології в галузі: навчальний посібник. Вінниця: ВНАУ. 2020. 253 с.
4. Полное руководство новичка по UX исследованию. 05.06.2018. URL: https://cutt.ly/KBh3za5
5. Дослідження UX: все про цілі, методи, специфіку. 17.09.2020. URL: https://luxnet.io/uk/blog/ux-research-ua
6. UX-исследования: процесс, методы, инструменты: конспект лекции Product designer в Prequel Никиты Шишкина – о том, как понять пользователя. 13.12.2021. URL: HTTPS://SKVOT.IO/RU/BLOG/UX-ISSLEDOVANIYA-PROCESS-METODY-INSTRUMENTY

УДК 004.6

СИСТЕМИ УПРАВЛІННЯ СИМЕТРИЧНИМИ ТА АСИМЕТРИЧНИМИ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ

К. К. Колосова, П. В. Римар

Анотація. Стаття присвячена порівнянню симетричних та асиметричних криптографічних ключів. У роботі наведено переваги та недоліки криптографічних ключів. Наведені приклади шифрування, криптографії і схеми симетричної та асиметричної криптосистеми.

Ключові слова: криптографія, шифрування, симетричні ключі, асиметричні ключі.

Вступ. Інформація є одним із найцінніших ресурсів будь-якої організації чи державної установи, тому забезпечення захисту інформації є однією з найважливіших і пріоритетних завдань. Безпека інформаційної системи – це властивість, яка втілює здатність системи забезпечити її нормальне функціонування, тобто забезпечити цілісність і секретність інформації.

Для забезпечення цілісності й конфіденційності інформації необхідно забезпечити захист інформації від випадкового знищення або несанкціонованого доступу до неї [1]. Цілісністю вважається неможливість несанкціонованого або випадкового знищення, а також модифікації інформації. Конфіденційність інформації – неможливість витоку і несанкціонованого заволодіння, зберігання інформації, яка передається чи приймається. Наука, яка вивчає математичні методи захисту інформації шляхом її перетворення, називається криптологією. Криптологія має два напрями – криптографію та криптоаналіз.

Основна частина. Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одними з головних задач якої є забезпечення конфіденційності, цілісності й автентичності даних, що передаються [2, с. 5].

Для забезпечення безпеки інформаційних систем застосовують системи захисту інформації, тобто комплекс організаційно-технологічних заходів, програмно-технічних засобів і правових норм, спрямованих на протидію джерелам загроз безпеці інформації. Захист інформації – це сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умови впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації [3].

До засобів захисту інформації інформаційної системи від дій суб'єктів належать:

- засоби захисту інформації від несанкціонованого доступу;
- захист інформації в комп'ютерних мережах;
- криптографічний захист інформації;
- електронний цифровий підпис;
- захист інформації від комп'ютерних вірусів.

Припускають, що шифрування з'явилося приблизно 4 тис. років тому. Першою відомою пам'яткою шифрування прийнято вважати єгипетський текст, який було створено приблизно в 1900 році до нашої ери, у якому використовувались інші символи замість відомих єгипетських ієрогліфів. Шифрування – це зворотне перетворення даних із метою приховування інформації. Шифрування відбувається із застосуванням криптографічного ключа. Ключ – це певна кількість символів, сформованих у вільний спосіб, що доступні у системі шифрування.

Криптографія – наука про математичні методи забезпечення конфіденційності, цілісності та автентичності інформації. Розвиток її розпочався з практичної потреби передавати важливі відомості найнадійнішим способом. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей. На першому етапі розвитку криптографії існувало два основні типи перетворень відкритих текстів – заміни й перестановки. Шифрів перестановки відомо достатньо велика кількість – зокрема, це й шифр «скітала», який шифрує таблиці та інше. Головна ідея шифрів перестановки є заміна місця розташування символів відкритого тексту. Шифрів заміни було значно більше, але всі вони будувалися на заміні символу відкритого тексту символом зашифрованого тексту. До таких шифрів належать квадрат Полібія, таблиці Трисемуса, система шифрування Віжінера та інші.

На другому етапі передбачалося, що для шифрування й розшифрування використовується один секретний ключ. Ці системи були названі симетричними. Як було сказано вище, основними принципами шифрування стають розсіювання й перемішування. Відповідно до розвитку криптографії в симетричних криптографічних системах виділяються два основних напрями шифрування: блокові й потокові шифри. Наступним більшим класом є асиметричні криптографічні системи, або системи з відкритим ключем. Головною ідеєю під час створення цього класу шифрів є генерація двох ключів. Один відкритий ключ поширюється по відкритих каналах зв'язку й використовується для шифрування повідомлень. На приймаючій стороні за допомогою секретного ключа проводиться розшифрування повідомлення. Основою під час створення таких шифрів, як сказано вище, є задачі зі складним розв'язком. Такими задачами у цей час є задачі факторизації, дискретного логарифмування й методи теорії завадостійкого кодування. Класифікацію алгоритмів шифрування представлено на рис 1.1 [4]:

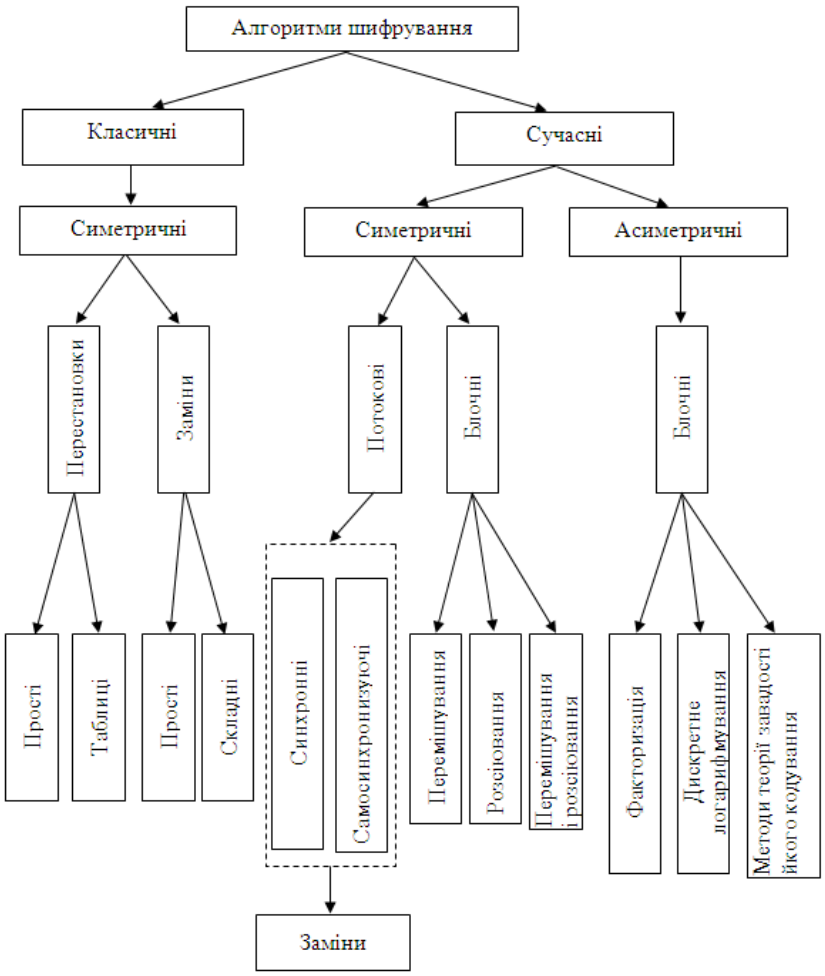

Рис. 1 – Класифікація алгоритмів шифрування

Метод симетричного шифрування (розшифрування) – це метод, за яким ключі шифрування і розшифрування є або однаковими, або легко обчислюються один з одного, забезпечуючи спільний ключ, який є таємним [9]. До симетричних алгоритмів шифрування належать: Twofish, Serpent, AES (або Рейндайль), Blowfish, CAST5, RC4, TDES (3DES) та IDEA. До основних асиметричних алгоритмів шифрування належать RSA та ECC.

Асиметричне шифрування, або метод відкритого ключа, передбачає застосування в парі двох відмінних ключів, а саме секретного та відкритого. Відповідно до назви, відкритий ключ безперешкодно розміщується у мережі; логічно, що секретний ключ весь час тримається в таємниці. В асиметричному шифруванні ключі співпрацюють у парі, тобто коли інформація шифрується відкритим ключем, розшифровування відбувається тільки відповідним секретним ключем та навпаки. Неможливим є використання відкритого ключа з однієї пари та секретного ключа з іншої пари. Математичними залежностями пов’язані всі пари асиметричних ключів.

Усі системи управління симетричними ключами, незалежно від того, скільки учасників задіяно в процесі, класифікуються насамперед на системи, в яких між суб’єктами вже встановлені захищені канали (тобто присутні секретні майстер-ключі), і на системи, в яких цього каналу немає.

Наприклад, відправник генерує відкритий текст вихідного повідомлення, яке повинно бути передано законному одержувачу незахищеним каналом. За каналом стежить перехоплювач із метою перехопити і розкрити передане повідомлення. Для того, щоб перехоплювач не зміг дізнатися змісту повідомлення, відправник шифрує його за допомогою оборотного перетворення і отримує шифротекст (або криптограму), який відправляє одержувачу. Законний одержувач, прийнявши шифр-текст, розшифровує його за допомогою зворотного перетворення і отримує вихідне повідомлення у вигляді відкритого тексту:

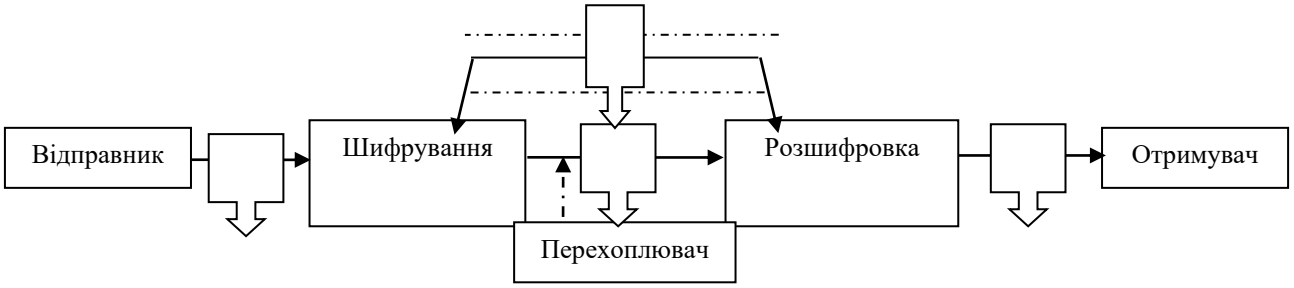

Рис. 2 – Схема симетричної криптосистеми з одним ключем

Асиметричні криптографічні системи були розроблені в 1970-х роках. Принципова відмінність асиметричної криптосистеми від криптосистеми симетричного шифрування полягає в тому, що для шифрування інформації та її подальшого розшифрування використовуються різні ключі:

– відкритий ключ використовується для шифрування інформації, обчислюється з секретного ключа;

– секретний ключ використовується для розшифрування інформації, зашифрованої за допомогою парного йому відкритого ключа.

Ці ключі розрізняються так, що за допомогою обчислень не можна вивести секретний ключ із відкритого ключа. Тому відкритий ключ може вільно передаватися каналами зв'язку. Асиметричні системи називають також двохключові криптографічні системи, або криптосистемами з відкритим ключем. Узагальнена схема асиметричної криптосистеми шифрування з відкритим ключем показана на рис. 3:

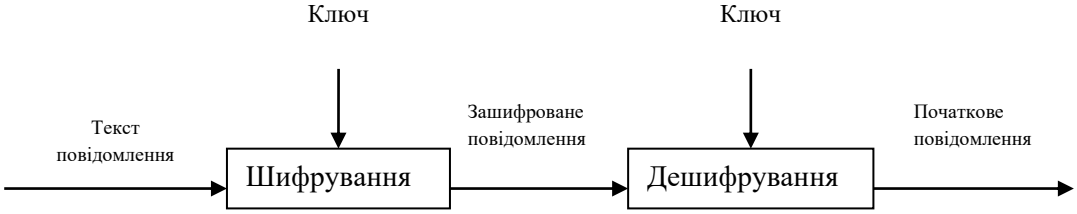

Рис. 3 – Схема асиметричної криптосистеми шифрування з відкритим ключем

Для криптографічного закриття і подальшого розшифрування переданої інформації використовуються відкритий і секретний ключі одержувача у повідомленні. Як ключ зашифровування повинен використовуватися відкритий ключ одержувача, а як ключ розшифрування – його секретний ключ. Секретний і відкритий ключі генеруються попарно. Секретний ключ повинен залишатись у його власника і бути надійно захищений від НСД (аналогічно до ключа шифрування в симетричних алгоритмах). Копія відкритого ключа повинна знаходитись у кожного абонента криптографічного мережі, з яким обмінюється інформацією власник секретного ключа.

У симетричному шифруванні можна виділити деякі переваги, наприклад, велика пропускна здатність завдяки спеціальному проєктуванню; ключі мають невеликий розмір; шифри можна застосовувати як основу для будування різноманітних криптографічних механізмів, зокрема і з випадковими генераторами чисел, обчислювально-ефективними схемами розпису тощо [5]. Серед недоліків цього шифрування слід відзначити те, що у кожній немаленькій мережі необхідно використовувати значну кількість ключів; за умов зв'язку між декількома особами необхідно досить часто змінювати ключі; коли існує зв'язок між двома особами, ключ слід засекречувати на двох кінцях.

Отже, ефективнішими є асиметричні криптосистеми, які ще по-іншому називаються криптосистемами з відкритим ключем. У таких системах для шифрування даних використовується один ключ, а для розшифрування – інший ключ (звідси і назва –асиметричні).

Висновки. Криптографія сьогодні – це найважливіша частина всіх інформаційних систем: від електронної пошти до стільникового зв'язку, від доступу до мережі Internet до елект-

ронної готівки. Криптографія забезпечує підзвітність, прозорість, точність та конфіденційність. Вона запобігає спробам шахрайства в електронній комерції та забезпечує юридичну силу фінансових транзакцій. Криптографія допомагає встановити вашу особу, але й забезпечує вам анонімність. Криптографічні методи захисту забезпечують неможливість несанкціонованого доступу, зміни або видалення важливих комерційних та особистих даних, що зберігаються на вашому комп'ютері. У світі сучасної комерції інформація є одним із найважливіших елементів, і основна частина цієї важливої інформації зберігається та обробляється в електронному вигляді, тому надійні методи захисту комп'ютерної інформації – це найкращий спосіб перешкодити навмисному або випадковому витоку.

Для того, щоб правильно реалізувати власну криптосистему, необхідно не тільки ознайомитися з помилками інших і зрозуміти причини, через які вони відбулися, а й, можливо, застосувати особливі захисні прийоми програмування та спеціалізовані засоби, розробки. На забезпечення комп'ютерної безпеки витрачаються мільярди доларів, причому більшість грошей викидається на непридатні продукти.

Abstract. The article is devoted to the comparison of symmetric and asymmetric cryptographic keys. The work indicates the advantages and disadvantages of cryptographic keys. Examples of encryption and cryptography and schemes of symmetric and asymmetric cryptosystems are given.

Keywords: cryptography, encryption, symmetric keys, asymmetric keys.

СПИСОК ЛІТЕРАТУРИ

1. Римар П. В., Крохмалюк В. В. Атаки на стеганосистеми. Криптографічні атаки. *Матеріали наукової конференції професорсько-викладацького складу, наукових працівників і здобувачів наукового ступеня за підсумками науково-дослідної роботи за період 2019–2020 рр. (квіт.–трав. 2021 р.).* Вінниця: ДонНУ імені Василя Стуса, 2021. С. 344–346.
2. Каткова Т. І. Забезпечення криптографічного захисту державних інформаційних ресурсів. *Наукові нотатки.* Луцьк. 2022. № 73. С. 54–58.
3. Карачка А. Ф. Технології захисту інформації: текст лекцій. Тернопіль, ТНЕУ, 2017. 86 с.
4. Криптографія та захист інформації. URL: 28.10.2018. https://studfile.net/preview/7013904/page:2/
5. Види шифрування інформації. URL: https://ua5.org/protect/395-vidi-shifruvannya-informaciyi.html

УДК 331.54:303.823-057.17]:[004.738.5:658.114.2

РОЛЬ ПРОДАКТ-МЕНЕДЖЕРА В ІТ-КОМПАНІЇ

С. Р. Корсовська, О. В. Зелінська

Анотація. Сучасні роботодавці хочуть, щоб кандидат на посаду продакт-менеджера був комунікабельним, організованим, здатним приймати рішення самостійно, нестандартно мислити та знати іноземну мову. Бажаним також є технічний досвід. Власне, проєкт-менеджери є важливим складником бізнес-процесу в ІТ. Вони є «містками-тлумачами» між чистими технічними спеціалістами та менеджментом компанії. Тому необхідно ознайомитися з професією продакт-менеджера, і розглянути можливості осягнути цей фах. У статті акцентовано на сутності роботи продакт-менеджера.

Ключові слова: продакт-менеджер, бізнес, ІТ, Product Manager.

Вступ. Продакт-менеджер – проміжний менеджер, який відповідає за низку завдань з управління та маркетингу. Вони відповідають за підтримку та маркування наявних продуктів, а також запуск нових продуктів певної лінійки, бренду чи послуги. Тобто продакт-менеджер управляє всім процесом з нуля до його завершення: він відповідає за створення, виведення на ринок та підтримку нового проєкту, вигадує, планує, створює, запускає та вдосконалює продукт.

Головна мета продакт-менеджера – створити прибутковий продукт, що відповідатиме очікуванням та потребам користувачів. Для цього вони повинні займатися плануванням і впровадженням продукту протягом усього життєвого циклу продукту. Продакт-менеджер є зв'язком між функціональними відділами в компанії, які займають кілька посад, наприклад, бренд-менеджер, галузевий менеджер або менеджер споживчого сегменту.