Course: Digital Financial Platforms and FinTech Systems

Lecture 9. Cybersecurity and Data Protection in FinTech Systems

Lecturer: Polishchuk Inna, PhD.

Курс: Цифрові фінансові платформи та FinTech-системи

Лекція 9. Кібербезпека та захист даних у FinTech-системах

Лектор: Поліщук Інна, PhD.

Зміст

- Кіберзагрози у FinTech-системах та їх специфіка
- Криптографічний захист даних у FinTech-платформах
- Управління цифровою ідентичністю та багатофакторна автентифікація
- Захист API, мобільних застосунків і хмарної інфраструктури у FinTech
- Управління інцидентами кібербезпеки та цифрова стійкість FinTech-систем
- Правові, етичні та комплаєнс-аспекти захисту даних у FinTech

01

Кіберзагрози у FinTech-системах та їх специфіка

Source: developed by the author

Кіберзагрози у FinTech-системах є сукупністю цифрових впливів, атак, уразливостей і зловмисних дій, які можуть порушити конфіденційність, цілісність, доступність або достовірність фінансових даних і сервісів. У середовищі FinTech ці загрози мають особливу значущість, оскільки цифрові фінансові платформи працюють із грошовими потоками, персональними даними, цифровою ідентичністю користувача, платіжними інструментами та критично важливими транзакційними процесами [1-2].

Однією з найпоширеніших груп загроз є **атаки на облікові дані та цифрову ідентичність**. До них належать фішинг, викрадення паролів, перехоплення одноразових кодів, підміна сторінок входу, компрометація сесій і несанкціоноване використання токенів доступу. У FinTech-системах такі атаки є особливо небезпечними, оскільки доступ до акаунта часто фактично означає доступ до фінансових операцій, платіжних інструментів і персоналізованих сервісів.

Окрему категорію становлять **атаки на мобільні FinTech-застосунки.** Мобільний клієнт є однією з основних точок взаємодії користувача з фінансовою системою, тому компрометація цього рівня створює безпосередню загрозу для транзакційної безпеки. До таких атак належать реверс-інжиніринг застосунку, ін’єкція шкідливого коду, перехоплення даних у небезпечному середовищі, підміна сертифікатів, емуляція пристрою та використання шкідливих програм для читання повідомлень або захоплення екрана.

Особливу складність становлять **атаки на бізнес-логіку фінансових сервісів.** На відміну від класичних технічних зламів, у цьому випадку зловмисник використовує не стільки вразливість програмного коду, скільки слабкі місця у правилах роботи системи. Це може бути повторне використання транзакційного сценарію, обхід обмежень на операції, маніпуляція порядком виконання дій, використання часових вікон, некоректне комбінування функцій платформи або ініціювання операцій у нестандартній послідовності.

Узагальнено специфіку кіберзагроз у FinTech можна подати через кілька ключових ознак: висока мотивація зловмисника, прямий зв’язок із грошовими активами, залежність від цифрової ідентичності, критичність API-взаємодії, уразливість мобільного середовища, можливість атак на бізнес-логіку та швидке перетворення кіберінциденту на фінансовий збиток.

Тип кіберзагрози	Сутність	Типовий наслідок у FinTech
Атаки на облікові дані	викрадення паролів, токенів, сесій	несанкціонований доступ до акаунта
API-атаки	зловживання інтерфейсами, обхід авторизації	витік даних, підміна запитів, обхід логіки
Атаки на мобільні застосунки	компрометація клієнтського середовища	перехоплення даних, підміна дій користувача
Атаки на доступність	перевантаження сервісів, DDoS	порушення роботи платформи, затримки операцій
Атаки на бізнес-логіку	маніпуляція сценаріями роботи системи	некоректні транзакції, обхід обмежень

Source: developed by the author based on [1].

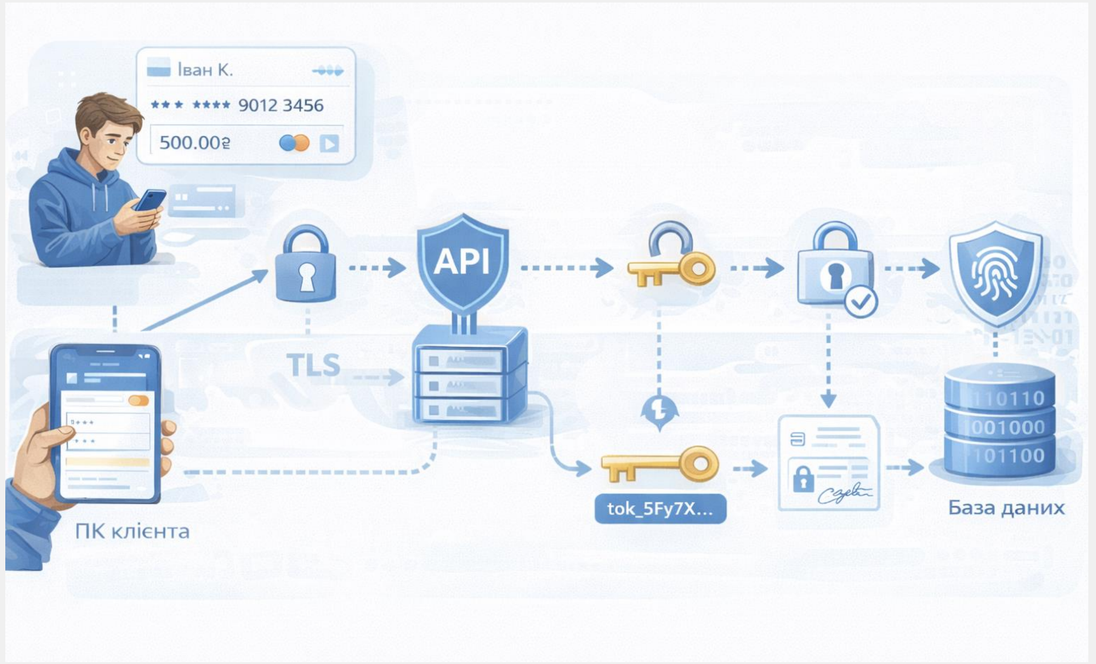
Приклад

Source: developed by the author

Наведений приклад демонструє, що в **FinTech-системах** навіть одна кіберзагроза може поєднувати елементи соціальної інженерії, технічної компрометації та фінансового шахрайства. Саме тому захист у такому середовищі має охоплювати не лише серверну інфраструктуру, а й **акаунти користувачів, мобільні застосунки, механізми автентифікації та поведінковий моніторинг.**

02

Криптографічний захист даних у FinTech-платформах



Source: developed by the author

Криптографічний захист даних у FinTech-платформах є фундаментальним механізмом забезпечення **конфіденційності, цілісності та автентичності фінансової інформації.** У цифровому фінансовому середовищі криптографія використовується для захисту транзакцій, зберігання персональних даних, підтвердження особи користувача та забезпечення довіри між взаємодіючими сторонами [2].

Асиметричні алгоритми базуються на використанні пари ключів – відкритого і закритого. До найбільш відомих належать **RSA, ECC (Elliptic Curve Cryptography) та алгоритми на основі кривих Едвардса.** У FinTech-платформах асиметрична криптографія використовується для обміну ключами, цифрового підпису та встановлення захищених каналів зв’язку. Зокрема, протоколи типу **TLS (Transport Layer Security)** поєднують асиметричні алгоритми для початкового узгодження ключів із симетричними алгоритмами для швидкої передачі даних.

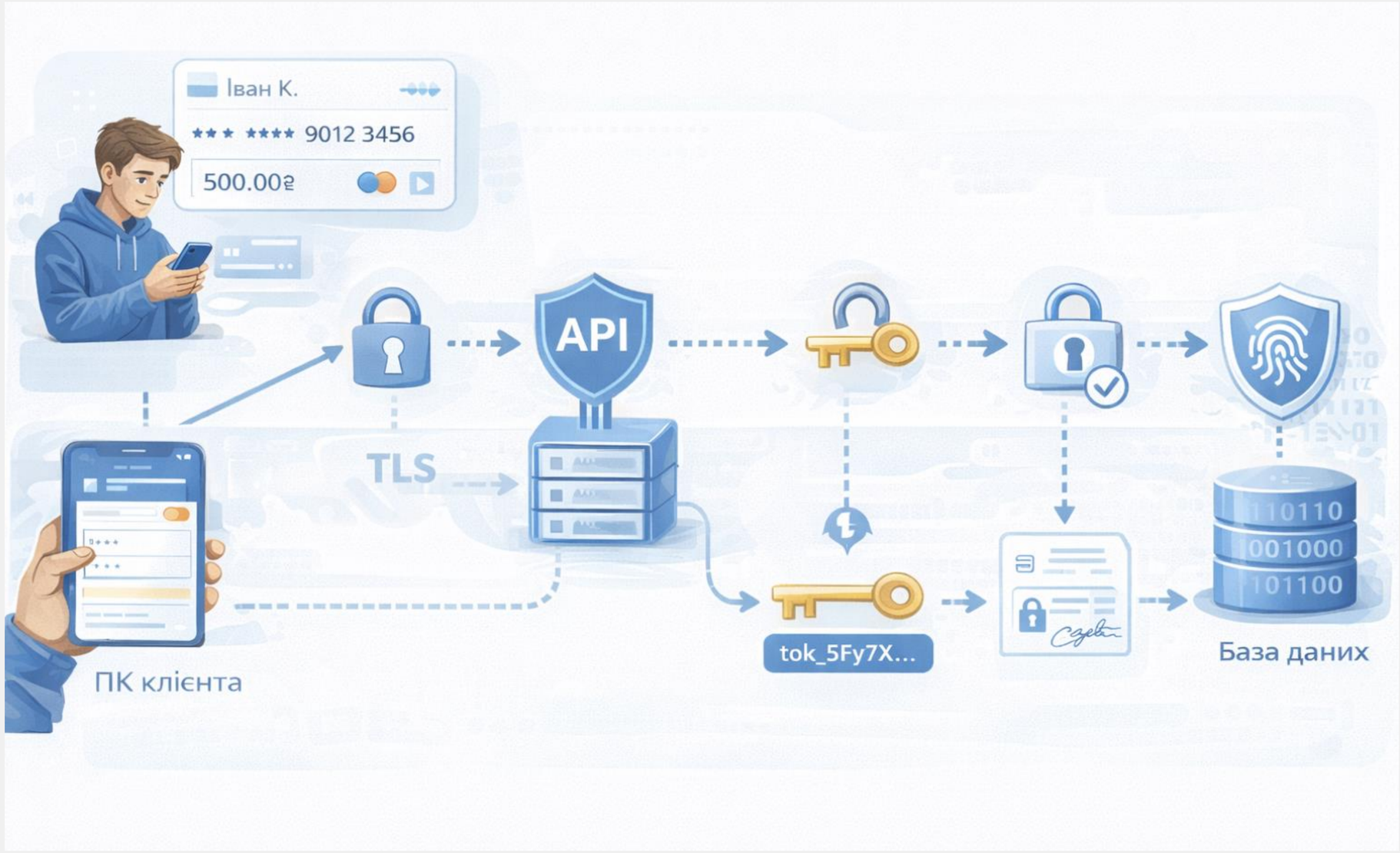
Окрему роль відіграє **цифровий підпис,** який дозволяє підтвердити автентичність і незмінність даних. У фінансових операціях цифровий підпис застосовується для підтвердження транзакцій, укладення електронних договорів, взаємодії з банківськими API та забезпечення юридичної значущості електронних документів. Найпоширеними алгоритмами є **RSA-PSS, ECDSA** та сучасні схеми на основі кривих **Едвардса**, що забезпечують високу ефективність і безпеку.

У сучасних FinTech-рішеннях широко застосовуються **протоколи управління ключами та інфраструктура відкритих ключів** (PKI). Управління ключами включає генерацію, розподіл, зберігання, ротацію та відкликання ключів. Для цього використовуються апаратні засоби, такі як **HSM (Hardware Security Module),** які забезпечують захищене середовище для виконання криптографічних операцій. Належна організація життєвого циклу ключів є критично важливою, оскільки компрометація ключа може звести нанівець усі інші механізми захисту.

Тип криптографії	Алгоритми	Призначення у FinTech
Симетрична	AES, ChaCha20	швидке шифрування даних і транзакцій
Асиметрична	RSA, ECC, Ed25519	обмін ключами, цифровий підпис
Хеш-функції	SHA-256, SHA-3, Argon2	зберігання паролів, перевірка цілісності
Цифровий підпис	ECDSA, RSA-PSS	підтвердження транзакцій
Токенізація	–	захист платіжних даних

Source: developed by the author based on [2].

Практичний сценарій (case study)



Source: developed by the author

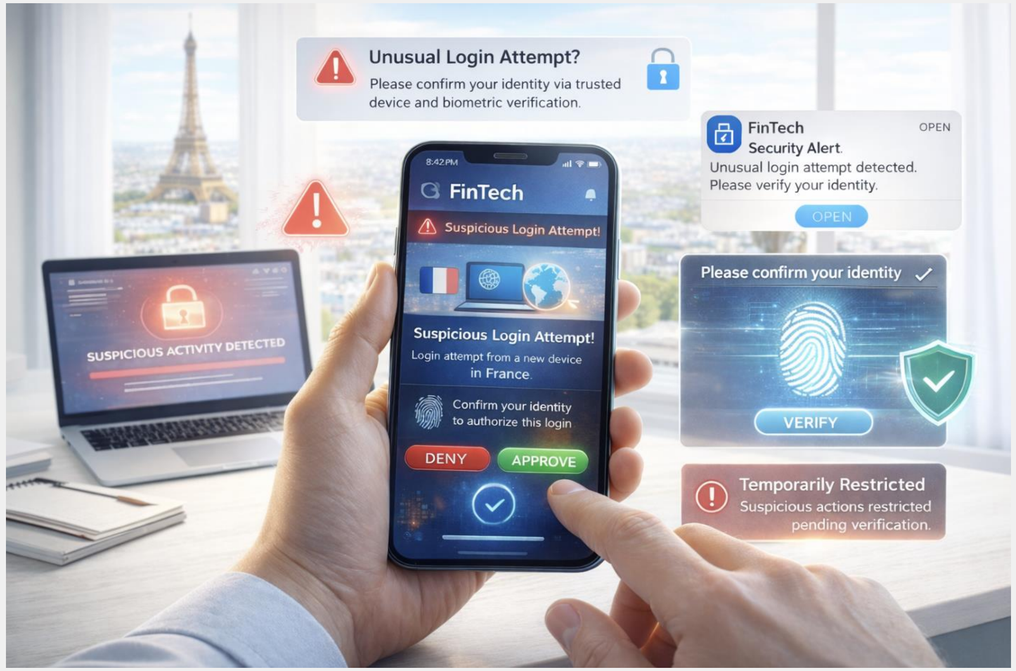
Моделі безпеки у FinTech-платформах

У сучасних FinTech-системах криптографічні алгоритми реалізуються в межах більш широких **моделей безпеки,** які визначають принципи організації захисту. Однією з ключових є модель **Zero Trust,** відповідно до якої жоден користувач або компонент системи не вважається довіреним за замовчуванням. Кожен запит до системи проходить перевірку автентичності, авторизації та контексту доступу незалежно від того, чи надходить він із внутрішнього або зовнішнього середовища [2].

Ще одним перспективним напрямом є **Confidential Computing**, який передбачає обробку даних у зашифрованому вигляді навіть під час виконання обчислень. Це досягається шляхом використання захищених середовищ виконання (Trusted Execution Environments), що дозволяє мінімізувати ризик витоку даних навіть у разі компрометації інфраструктури.

03

Управління цифровою ідентичністю та багатофакторна автентифікація



Source: developed by the author

Управління цифровою ідентичністю у FinTech-системах є сукупністю методів, правил і технологічних механізмів, які забезпечують створення, перевірку, підтримку та контроль цифрового представлення користувача в інформаційному середовищі. У фінансових платформах цифрова ідентичність охоплює не лише обліковий запис, а й набір атрибутів, що підтверджують особу, права доступу, історію взаємодії, довірені пристрої та ознаки поведінки користувача [3].

Класичний підхід до перевірки особи базується на використанні одного фактора, найчастіше **пароля**. Однак у цифровому фінансовому середовищі такий механізм є недостатнім, оскільки паролі можуть бути викрадені, вгадані, перехоплені або повторно використані. Саме тому широкого поширення набуває **багатофакторна автентифікація** (MFA), тобто перевірка користувача на основі двох або більше незалежних факторів.

У сучасних FinTech-платформах важливого значення набуває **адаптивна автентифікація**, за якої рівень перевірки користувача залежить від контексту доступу. Система може враховувати геолокацію, тип пристрою, час входу, IP-адресу, характер дій, історію попередніх сесій та інші параметри цифрової поведінки. Якщо вхід відповідає типовому шаблону, перевірка може бути спрощеною. Якщо ж виявляються аномальні ознаки, система активує додатковий рівень захисту, наприклад повторне підтвердження особи або тимчасове обмеження доступу.

Архітектурно управління цифровою ідентичністю реалізується через спеціалізовані сервіси **IAM (Identity and Access Management),** модулі автентифікації, сховища атрибутів, системи управління сесіями та журнали подій безпеки. У межах таких систем підтримуються ролі користувачів, політики доступу, токени сесій, механізми Single Sign-On, протоколи OAuth 2.0, OpenID Connect та інші засоби контрольованої взаємодії між користувачем і платформою.

Приклад

Source: developed by the author

04

Захист API, мобільних застосунків і хмарної інфраструктури у FinTech

Source: developed by the author

У сучасних FinTech-системах безпека є невід’ємною складовою архітектури цифрових сервісів, оскільки саме вона забезпечує конфіденційність фінансових даних, цілісність транзакцій і безперервність функціонування платформи. Особливого значення набуває захист **API, мобільних застосунків і хмарної інфраструктури**, адже ці компоненти формують основу більшості фінансово-технологічних рішень [4].

Одним із ключових аспектів є організація **автентифікації та авторизації API-запитів.** У практиці сучасної розробки для цього широко застосовуються **OAuth 2.0, OpenID Connect, JWT-токени**, а також взаємна автентифікація на основі сертифікатів. Безпечне API повинно чітко визначати, хто саме ініціює запит, які права доступу має клієнт, до яких ресурсів він може звертатися і протягом якого часу зберігається чинність доступу. Не менш важливою є валідація вхідних даних, оскільки некоректно перевірені параметри можуть відкрити шлях до атак типу SQL injection, command injection або до експлуатації логічних помилок прикладного рівня.

Архітектура безпечного мобільного застосунку передбачає винесення критично важливої бізнес-логіки на серверний бік. Операції, пов’язані з валідацією транзакцій, перевіркою правил доступу, аналізом ризику та прийняттям рішень, не повинні реалізовуватися виключно на стороні клієнта, оскільки це створює можливості для обходу механізмів контролю. Мобільний застосунок має виконувати насамперед функції інтерфейсу взаємодії, безпечної передачі запитів і відображення результатів. Додатковий рівень захисту забезпечують **сертифікатний pinning, багатофакторна автентифікація, контроль сесій, обмеження ризикових дій і механізми виявлення аномальної поведінки.**

Функціонування FinTech-платформи в хмарі ґрунтується на моделі **shared responsibility**, тобто розподіленої відповідальності між постачальником хмарних послуг і організацією, яка використовує відповідне середовище. Постачальник відповідає за фізичну безпеку дата-центрів, базову інфраструктуру та доступність платформних сервісів, тоді як організація відповідає за правильне налаштування політик доступу, захист прикладного рівня, класифікацію даних, управління ідентичностями та дотримання внутрішніх вимог безпеки.

05

Управління інцидентами кібербезпеки та цифрова стійкість FinTech-систем

Source: developed by the author

У сучасних **FinTech-системах** питання кібербезпеки не обмежується лише запобіганням атакам, а охоплює також здатність системи своєчасно виявляти порушення, реагувати на них і відновлювати нормальне функціонування. Саме тому важливими поняттями стають **інцидент кібербезпеки** та **цифрова стійкість.** Під інцидентом кібербезпеки розуміють будь-яку подію, яка призводить або може призвести до порушення конфіденційності, цілісності чи доступності інформації та цифрових сервісів [5].

Ключовим етапом у роботі з інцидентами є їх **виявлення та класифікація.** Для цього в сучасних FinTech-рішеннях використовуються системи моніторингу мережевої активності, аналізу журналів, виявлення аномалій, кореляції подій та поведінкового аналізу користувачів і пристроїв. Виявлена подія повинна бути оцінена за рівнем критичності, джерелом походження, масштабом впливу та потенційними наслідками.

Після стримування загрози виконується **усунення причин інциденту та відновлення системи.** Усунення передбачає видалення шкідливого коду, виправлення вразливості, зміну скомпрометованих облікових даних, оновлення конфігурацій або посилення політик доступу. Відновлення, у свою чергу, спрямоване на повернення системи до нормального або контрольовано безпечного режиму роботи. У FinTech цей етап часто пов’язаний із відновленням транзакційних сервісів, повторною синхронізацією даних, перевіркою цілісності фінансових записів і контролем коректності взаємодії між модулями системи.

Поняття **цифрової стійкості** є ширшим за традиційне реагування на інциденти, оскільки воно охоплює здатність організації підтримувати критичні операції в умовах порушення, швидко адаптуватися до нових загроз і мінімізувати системний вплив атак. Цифрова стійкість у FinTech досягається через поєднання **відмовостійкої архітектури, резервування ресурсів, автоматизованого моніторингу, сегментації середовища, регулярного тестування сценаріїв збоїв**, а також чітких процедур комунікації під час кризових ситуацій.

Source: developed by the author

06

Правові, етичні та комплаєнс-аспекти захисту даних у FinTech

Source: developed by the author

У сучасних **FinTech-системах** захист даних є не лише технічним завданням, а й важливою **правовою, етичною та комплаєнс-функцією.** Це пояснюється тим, що фінансово-технологічні платформи працюють із великими обсягами персональних даних, платіжної інформації, ідентифікаційних відомостей, поведінкових профілів користувачів та історії транзакцій. Будь-яка помилка в роботі з такими даними може мати наслідком не лише порушення безпеки, але й юридичну відповідальність, репутаційні втрати та зниження довіри клієнтів [6].

Окремого значення набуває **поняття персональних даних і чутливої інформації.** У FinTech до персональних даних належать не лише ім’я, адреса чи номер документа, а й банківські реквізити, історія платежів, геолокаційні ознаки, цифрові ідентифікатори, IP-адреси, відомості про фінансову поведінку користувача та інші атрибути, за якими особу можна прямо або опосередковано ідентифікувати. Це вимагає застосування принципів мінімізації **даних, обмеження мети обробки, точності, конфіденційності та контрольованого доступу**.

Етична проблематика також пов’язана з питанням **цифрової довіри.** Користувач повинен розуміти, які саме дані про нього збираються, для чого вони потрібні, як довго зберігаються та які наслідки може мати їх обробка. Якщо система використовує **штучний інтелект, аналітику поведінки або автоматизоване профілювання,** виникає потреба забезпечити не лише точність алгоритмів, а й пояснюваність їх результатів.

Третім важливим виміром є **комплаєнс,** тобто система внутрішнього забезпечення відповідності діяльності організації зовнішнім нормативним вимогам і внутрішнім політикам. У сфері FinTech **комплаєнс-захист даних** охоплює політики доступу, регламенти обробки інформації, процедури аудиту, контроль зберігання журналів подій, управління інцидентами, перевірку контрагентів та документування операцій із даними.

У структурі комплаєнсу особливого значення набувають управління доступом, розмежування ролей, аудит дій користувачів і адміністраторів, а також контроль відповідності процесів життєвому циклу даних.

Правові, етичні та комплаєнс-аспекти захисту даних у FinTech слід розглядати як взаємопов’язані складові єдиної моделі відповідального цифрового середовища. Право визначає рамки допустимої обробки даних, етика формує стандарти справедливого і прозорого ставлення до користувача, а комплаєнс забезпечує практичне впровадження цих вимог у діяльність організації та в архітектуру цифрової платформи.

Підсумок лекції

У лекції розглянуто основні засади кібербезпеки у FinTech-системах, зокрема питання цифрової ідентичності, багатофакторної автентифікації, захисту API, мобільних застосунків, хмарної інфраструктури, управління інцидентами та цифрової стійкості. Також увагу зосереджено на правових, етичних і комплаєнс-аспектах захисту даних, які є невід’ємною складовою сучасних фінансово-технологічних платформ.

Пропонована література

[1]. AlBenJasim, S., Al-Husaini, H., Naqvi, B., Al-Bastaki, Y., Al-Ali, W., Alawadhi, A., Hilal, N., Alsini, R., & Al-Qaidi, S. FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. Journal of Computer Information Systems, 2024.
Стаття систематизує основні кіберзагрози у FinTech, розглядає типові вразливості цифрових фінансових сервісів і показує зв’язок між технічними ризиками та регуляторними вимогами. Це доречне джерело для вступного параграфу лекції, де розкривається актуальність кібербезпеки у FinTech.

[2]. Temoshok, D., et al. NIST SP 800-63B-4: Digital Identity Guidelines — Authentication and Authenticator Management. National Institute of Standards and Technology, 2025.
Це сучасний навчально-нормативний матеріал, у якому визначено вимоги до цифрової автентифікації, рівнів надійності автентифікаторів, багатофакторної автентифікації та управління засобами підтвердження особи. Джерело добре підходить для пояснення принципів цифрової ідентичності у FinTech.

Пропонована література

[3]. OWASP Foundation. OWASP API Security Top 10 — 2023.
Цей навчальний матеріал містить актуалізований перелік найнебезпечніших ризиків безпеки API, серед яких порушення авторизації, проблеми автентифікації, надмірне розкриття даних і неконтрольоване споживання ресурсів. Джерело доцільно використати для пояснення загроз і базових принципів захисту API у фінансово-технологічних системах.

[4]. OWASP Foundation. Mobile Application Security Verification Standard (MASVS) v2.1.0. 2024.
Це один із найавторитетніших навчальних стандартів для безпеки мобільних застосунків. У ньому подано вимоги до захисту мобільного коду, зберігання даних, криптографії, мережевої взаємодії, автентифікації та приватності. Джерело є особливо корисним для розкриття теми безпечної розробки мобільних FinTech-застосунків.

Пропонована література

[5]. Nelson, A., et al. NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management. National Institute of Standards and Technology, 2025.
У цьому навчально-методичному документі подано сучасний підхід до підготовки, виявлення, аналізу, реагування та відновлення після інцидентів кібербезпеки. Матеріал доречний для пояснення етапів реагування на інцидент і формування цифрової стійкості FinTech-систем.

[6]. Dorfleitner, G., Hornuf, L., & Kreppmeier, J. Promise not fulfilled: FinTech, data privacy, and the GDPR. Electronic Markets, 2023, 33:33.
Стаття аналізує, як GDPR вплинув на політики конфіденційності FinTech-компаній, зокрема на зміст і зрозумілість повідомлень про обробку даних. Це релевантне наукове джерело для розкриття правових і комплаєнс-аспектів захисту персональних даних у FinTech.

Дякую за увагу!