УДК 004.45

ОСОБЛИВОСТІ ІНТЕГРАЦІЇ СИСТЕМ ЗАХИСТУ ДАНИХ У ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ: ВІД КОНЦЕПЦІЇ ДО ВПРОВАДЖЕННЯ

Людмила Глинчук, Софія Лапчук

FEATURES OF DATA PROTECTION SYSTEMS INTEGRATION INTO SOFTWARE: FROM CONCEPT TO IMPLEMENTATION

Liudmyla Hlynchuk, Sofiia Lapchuk

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This study explores the integration of data protection systems into software throughout its lifecycle, from concept to implementation. It focuses on the Ukrainian "Diia" app, demonstrating the "security by design" approach, where security is embedded from the start. The research emphasizes the importance of continuous integration to ensure effective protection against cyber threats.*

Із зростанням обсягу цифрових послуг та переходом до моделі «держава в смартфоні», критично зростає значення інтеграції систем захисту даних у програмне забезпечення. Застарілі підходи, коли безпеку додають наприкінці розробки, вже не є ефективними в умовах постійних кіберзагроз. Відтак, актуальним є дослідження комплексних підходів до впровадження безпеки на всіх етапах створення програмних рішень.

Метою дослідження є аналіз особливостей інтеграції систем захисту даних у програмне забезпечення на прикладі реального українського досвіду реалізації таких систем, зокрема у застосунку «Дія».

Новизна полягає в комплексному розгляді процесу інтеграції систем захисту даних на всіх етапах життєвого циклу програмного забезпечення – від концептуального проєктування до практичного впровадження. Відповідно до рисунку 1 інтеграція повинна розпочинатися на етапі концепції.

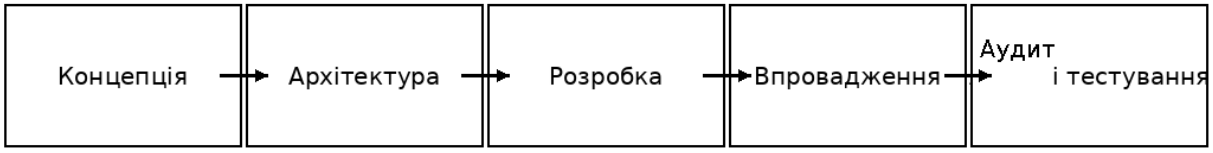

Рисунок 1. Схема інтеграції систем захисту у ПЗ

Опишемо коротко, що відбувається на кожному з етапів. І так, на етапі «Концепція» формуються базові вимоги до безпеки, вибираються моделі загроз, визначається загальний підхід до захисту даних. Наступний етап «Архітектура», тут безпека враховується при побудові логічної структури системи та визначаються точки контролю, способи шифрування, автентифікації тощо. Етап «Розробка» полягає в реалізації механізмів безпеки: шифрування, авторизація, аудит подій. На етапі «Впровадження» забезпечується безпечне розгортання, ізоляція середовищ, інтеграція з захищеними сервісами. І, нарешті, на етапі «Аудит і тестування» відбувається перевірка на вразливості, тестування на проникнення та відповідність стандартам. Таким чином, інтеграція систем захисту не є одноразовою дією – це безперервний процес. [1]

Аналіз інтеграції систем захисту даних доцільно проводити на прикладі українського державного застосунку «Дія», який став зразком реалізації підходу *security by design* у

публічному секторі. Security by design означає вбудовування механізмів захисту даних у програмне забезпечення ще на етапі його проєктування, а не як додатковий елемент після розробки. Це дозволяє державним цифровим сервісам, таким як «Дія», мінімізувати ризики витоку персональної інформації та забезпечити відповідність національним і міжнародним стандартам безпеки з самого початку.

На концептуальному рівні безпека була закладена ще на етапі проєктування архітектури: застосунок не зберігає персональних даних на своїх серверах або на пристрої користувача. Замість цього він здійснює захищене підключення до державних реєстрів (наприклад, Реєстру населення, Єдиного демографічного реєстру) та передає дані у вигляді тимчасових візуалізацій. Такий підхід відповідає принципу *privacy by design*, що суттєво знижує ризики несанкціонованого доступу чи витоку інформації [2].

На етапі технічної реалізації застосовано багаторівневу модель захисту. Кожна сесія передачі даних шифрується з використанням сертифікованих засобів криптографічного захисту інформації (КСЗІ), затверджених у Держспецзв'язку. Аутентифікація користувачів здійснюється через інтеграцію з системами BankID НБУ та іншими механізмами, що забезпечують підтвердження особи без передачі зайвих персональних даних [3]. Це дозволяє не тільки убезпечити доступ до персоналізованих сервісів, але й забезпечити високий рівень зручності для громадян.

На етапі впровадження та експлуатації системи реалізовано кілька важливих практик. По-перше, застосунок піддається періодичному незалежному тестуванню на вразливості (*penetration testing*) з боку провідних українських та міжнародних компаній, зокрема EPAM. У межах національних багбаунті-програм також залучаються етичні хакери, які допомагають виявити потенційні загрози до їх експлуатації [4].

По-друге, відповідність системи вимогам національного законодавства та стандартам у сфері інформаційної безпеки перевіряється через аудит, проведений Державною службою спеціального зв'язку та захисту інформації України. Це включає аудит політик безпеки, механізмів доступу, обробки інцидентів та резервного копіювання. У такий спосіб забезпечується наскрізний контроль безпеки – від концепції до практичного функціонування сервісу [5].

Інтеграція систем захисту даних у програмне забезпечення є складним багаторівневим процесом, який починається ще на етапі архітектурного проєктування. Приклад застосунку «Дія» демонструє ефективність підходу, за якого безпека розглядається не як додатковий компонент, а як базовий елемент функціонування. Комплексний підхід, нормативне підкріплення та прозора комунікація з громадськістю сприяють формуванню довіри користувачів і підвищенню кіберстійкості державних сервісів.

Бібліографія

1. Microsoft. Рекомендації щодо забезпечення життєвого циклу розробки. Microsoft Learn. URL: https://learn.microsoft.com/uk-ua/power-platform/well-architected/security/secure-development-lifecycle
2. «Дія в дії: як запущено державу в смартфоні» [Електронний ресурс]. – Режим доступу: https://mind.ua/publications/20207444-diya-v-diyi-yak-zapushcheno-derzhavu-v-smartfoni
3. Безпека мобільного застосунку Дія – офіційна інформація [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/news/bezpeka-mobilnogo-zastosunku-diya
4. «Дія» пройшла перевірку багбаунті та підтвердила безпечність застосунку [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/news/diya-proyshla-perevirku-bagbaunti-ta-pidtverdila-bezpechnist-zastosunku
5. Федоров М. «Дія» – один із найбезпечніших IT-продуктів, який створювався в Україні [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/news/diya-odin-iz-najbezpechnishih-it-produktiv-yakij-stvoryuvavsya-v-ukrayini-mihajlo-fedorov