УДК 004.056

Д. В. Остафійчук
Л. О. Майданевич

ВПЛИВ НОРМАТИВНИХ ВИМОГ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ ТА ТЕСТУВАННЯ ПРОГРАМНИХ ЗАСОБІВ

Вінницький національний технічний університет

Анотація.

В доповіді проаналізовано проблему узгодження правових норм у сфері інформаційної безпеки з технічними механізмами їх реалізації під час розроблення та тестування програмного забезпечення. З'ясовано, що законодавство оперує переважно загальними категоріями, які потребують спеціальної інтерпретації при реалізації їх вимог у програмних системах. Відтак, ключовим завданням при розробці є трансформація правових норм в конкретні вимоги до кібербезпеки програмного забезпечення. Окрему увагу приділено: ролі міжнародних стандартів і рекомендацій; інтеграції правових вимог та технічних методів тестування задля забезпечення інформаційної безпеки сучасних цифрових сервісів.

Ключові слова: інформаційна безпека, кібербезпека, тестування програмного забезпечення, захист персональних даних.

Abstract.

The report analyzes the problem of harmonizing legal norms in the field of information security with technical mechanisms for their implementation during the development and testing of software. It was found that the legislation operates mainly with general categories that require special interpretation when implementing their requirements in software systems. Therefore, the key task in the development is the transformation of legal norms into specific requirements for software cybersecurity. Special attention is paid to: the role of international standards and recommendations; the integration of legal requirements and technical testing methods to ensure the information security of modern digital services.

Keywords: information security, cybersecurity, software testing, personal data protection.

Вступ

Сьогодні створити програму це не лише написати працюючий код, а й зробити так, щоб вона не порушувала закони. Такі документи, як Закон України «Про захист персональних даних» [1] або європейський GDPR, вимагають, щоб безпека закладалася в додаток із самого початку. Тому робота QA-інженера (тестувальника) починається дуже рано. Сучасний фахівець із якості має перевіряти не тільки те, чи правильно працюють кнопки, а й чи відповідає програма вимогам закону щодо захисту інформації користувачів.

Результати дослідження

Головна складність у забезпеченні інформаційної безпеки полягає у величезній прірві між юридичною мовою та технічними реаліями [2]. Закони оперують абстрактними поняттями, такими як «права людини», «конфіденційність» або «недоторканність приватного життя». Натомість розробникам і тестувальникам потрібні чіткі технічні завдання: які алгоритми шифрування використовувати, як налаштувати базу даних та які обмеження виставити в коді. Тому головне завдання IT-команди – це перетворити ці загальні правові норми на конкретні критерії для програми, тобто на нефункціональні вимоги, які потім ляжуть в основу детальних тест-планів.

Найкраще цей процес переходу від букви закону до практичного тестування видно на прикладі популярних месенджерів, зокрема під час перевірки додатків на кшталт WhatsApp. З точки зору права, закон суворо гарантує людям таємницю листування та захист їхніх особистих даних від сторонніх осіб. Для команди розробки це правило автоматично перетворюється на жорстку нефункціональну вимогу: усі повідомлення мають передаватися виключно за допомогою наскрізного шифрування. Крім того, архітектура програми має бути побудована так, щоб відкриті тексти повідомлень ніколи не зберігалися у внутрішній пам'яті смартфона після завершення сесії спілкування.

Коли ця вимога потрапляє до рук QA-інженера, вона розбивається на низку конкретних практичних дій. Спочатку тестувальник проводить перевірку мережі: він штучно перехоплює трафік програми під час відправки повідомлення і переконується, що дані йдуть у зашифрованому вигляді, і зловмисник не зможе прочитати їх як звичайний текст. Далі йде обов'язковий етап перевірки локальної пам'яті (Local Storage). Спеціаліст має зайти у приховані системні папки додатку на телефоні, дослідити кеш та логи, щоб перевірити, чи не залишилися там паролі, токени авторизації або шматки переписки після того, як

користувач закрив програму. Окремим важливим кроком є тестування дозволів: QA-інженер ретельно перевіряє, чи програма правильно, вчасно і зрозуміло запитує в користувача згоду перед тим, як отримати доступ до камери, мікрофона або списку контактів.

Щоб не вигадувати такі перевірки з нуля і нічого не забути, тестувальники рідко покладаються лише на власну інтуїцію. Вони активно використовують міжнародні стандарти, наприклад, OWASP Top 10 [3]. Це своєрідна галузева шпаргалка – актуальний список найпоширеніших загроз та вразливостей веб- і мобільних додатків, який допомагає створити дійсно якісний тест-план. Використання таких стандартів [4] гарантує, що команда не пропустить критичні діри в безпеці, через які користувачі можуть втратити дані, а компанія-розробник – отримати серйозні штрафи за порушення закону.

Висновки

Проведений аналіз засвідчує, що однією з ключових проблем забезпечення інформаційної безпеки є необхідність трансформації загальних правових норм у конкретні технічні вимоги до програмного забезпечення. Юридичні категорії, пов'язані із захистом приватності, конфіденційності та персональних даних, повинні бути інтерпретовані розробниками та фахівцями з тестування у вигляді чітких нефункціональних вимог до архітектури системи, алгоритмів шифрування, механізмів автентифікації та управління доступом. На практиці це реалізується через впровадження технічних рішень, зокрема наскрізного шифрування, безпечного зберігання даних та коректного управління дозволами користувача. Важливу роль у забезпеченні належного рівня кіберзахисту відіграє системне тестування програмних продуктів, що включає аналіз мережевого трафіку, перевірку локального зберігання даних та контроль доступу до ресурсів пристрою. Використання міжнародних стандартів і рекомендацій дозволяє уніфікувати процеси тестування безпеки та мінімізувати ризики витоку інформації. Таким чином, ефективна кібербезпека вимагає інтеграції правових вимог і технічних механізмів їх практичної реалізації.

Отже, нормативно-правові акти з інформаційної безпеки прямо керують тим, як ми тестуємо програми. Сучасні QA-інженери повинні розуміти базові закони та вміти перетворювати їх на робочі чек-листи. Якісне тестування, побудоване на правових вимогах, допомагає знаходити вразливості ще до випуску продукту, захищаючи користувачів від витоку даних, а компанію-розробника від проблем із законом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 02.03.2026).
2. ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. URL: https://my-itspecialist.com/iso-iec-27001-2022-standard (дата звернення: 02.03.2026).
3. OWASP Top 10:2021. The Ten Most Critical Web Application Security Risks. OWASP Foundation. URL: https://owasp.org/Top10/ (дата звернення: 02.03.2026).
4. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо підвищення рівня кіберзахисту інформаційно-комунікаційних систем, 2022. URL: https://cip.gov.ua/ (дата звернення: 02.03.2026).

Остафійчук Дмитро Володимирович – студент групи 2БС-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: osdima48@gmail.com

Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Ostafichuk Dmutro – student of group 2BS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vdemcenko234@gmail.com

Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com