КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.852
УДК 004.62

Курій Євгеній Олегович
доктор філософії, асистент
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-3423-5655
yevhenii.o.kurii@lpnu.ua

Сусукайло Віталій Андрійович
доктор філософії, асистент
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0003-4431-9964
vitalii.a.susukailo@lpnu.ua

Єрофеєва Анна Сергіївна
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0001-3256-1019
anna.yerofeieva.kb.2021@lpnu.ua

Нестерюк Марта Едуардівна
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0006-4229-7019
marta.nesteriuk.kb.2021@lpnu.ua

АНАЛІЗ ВПЛИВУ ВИМОГ DIGITAL OPERATIONAL RESILIENCE ACT (DORA) НА ПРОЦЕС БЕЗПЕЧНОЇ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Анотація. У статті здійснено комплексний аналіз впливу Регламенту Європейського Союзу Digital Operational Resilience Act (DORA) на безпечний життєвий цикл розробки програмного забезпечення (Secure Software Development Life Cycle, Secure SDLC) у фінансовому секторі. В умовах стрімкої цифрової трансформації банківських, страхових та інвестиційних послуг, DORA формує нову обов'язкову нормативну основу цифрової операційної стійкості, що охоплює широкий спектр напрямів, зокрема управління ризиками, пов'язаними з інформаційно-комунікаційними технологіями (ІКТ), обов'язкове звітування про серйозні кіберінциденти, регулярне тестування безпеки, контроль постачальників ІТ-послуг, а також координацію обміну інформацією про загрози між суб'єктами фінансового ринку. У роботі детально розглянуто п'ять ключових вимог DORA, визначених у тексті Регламенту, з акцентом на їх послідовну інтеграцію в усі етапи Secure SDLC — від ініціалізації, планування, аналізу вимог і проєктування архітектури до реалізації, тестування, впровадження, технічної підтримки, модернізації та виведення з експлуатації. Окрема увага приділяється питанням впровадження інструментів автоматизованого тестування безпеки (SAST, DAST, IAST), використанню систем виявлення аномальної активності (SIEM, UEBA), впровадженню Software Bill of Materials (SBOM) для підвищення прозорості компонентів, а також розробці та впровадженню планів реагування на інциденти (IRP) і планів забезпечення безперервності бізнесу (BCP). Запропоновано таблицю узгодження ключових статей DORA з відповідними фазами життєвого циклу SDLC, що дозволяє ідентифікувати критичні точки відповідності, зменшити прогалини у безпеці та оптимізувати впровадження вимог цифрової стійкості. У дослідженні розглянуто сучасні підходи до інтеграції безпекових практик у CI/CD-процеси, важливість підвищення обізнаності працівників щодо актуальних кіберзагроз, а також формування культури безпеки, орієнтованої на проактивний захист навіть після розгортання ПЗ. Зазначається, що дотримання вимог DORA не слід розглядати виключно як відповідь на регуляторний тиск, а як основу для довгострокової трансформації корпоративної цифрової безпеки у фінансових установах. Результати дослідження становлять інтерес для розробників програмного забезпечення, спеціалістів з інформаційної безпеки, фахівців з управління ризиками, регуляторів та внутрішніх і зовнішніх аудиторів,

які прагнуть забезпечити відповідність новим нормативним вимогам і посилити цифрову стійкість організацій у високоризиковому середовищі.

Ключові слова: DORA; кіберстійкість; безпечна розробка програмного забезпечення; інформаційна безпека; управління ризиками; фінансові установи; моніторинг; управління інцидентами.

ВСТУП

В умовах стрімкого розвитку цифрових фінансових послуг, забезпечення операційної стійкості набуває першочергового значення. Закон про цифрову операційну стійкість (Digital Operational Resilience Act, DORA), прийнятий Європейським Союзом (ЄС), запровадив нову еру стандартів операційної стійкості для фінансових установ в ЄС, підкресливши важливість надійного управління ризиками інформаційно-комунікаційних технологій (ІКТ) та безпечних практик розробки програмного забезпечення.

Постановка проблеми. У сучасних умовах стрімкої цифровізації фінансового сектора навіть короткочасні збої ІТ-систем можуть призводити до значних фінансових та репутаційних втрат. Відсутність єдиної нормативної бази цифрової операційної стійкості довгий час залишалася прогалиною в регулюванні ІКТ-ризиків у Європейському Союзі. Регламент DORA вперше системно врегулював питання кіберстійкості фінансових установ, однак імплементація його вимог у процес розробки програмного забезпечення вимагає переосмислення методів захисту, інтеграції безпеки в Secure SDLC, а також підвищення рівня контролю над ризиками сторонніх постачальників. Попри детальний опис вимог DORA, залишаються відкритими питання ефективної адаптації цих вимог в умовах реальної розробки, тестування та супроводу ПЗ.

Аналіз останніх досліджень і публікацій. У Регламенті (ЄС) 2022/2554 [1], відомому як Digital Operational Resilience Act (DORA), встановлюється законодавча база цифрової операційної стійкості для фінансових установ та їхніх ІКТ-постачальників в Європейському Союзі. Даний регламент зобов’язує компанії відповідати стандартизованим вимогам безпеки для їхніх мереж та інформаційних систем з метою захисту від кібератак, а також гарантувати здатність протистояти, реагувати та відновлюватися після всіх видів збоїв і загроз, пов’язаних з ІКТ. Це дослідження підкреслює важливість створення єдиних правил для запобігання та пом’якшення кіберзагроз у фінансовому секторі ЄС.

У публікації [2] розглядаються ключові аспекти підготовки до впровадження вимог DORA, фокусуючись на п’яти основних стовпах відповідності: управлінні ІКТ-ризиками, звітуванні про інциденти, тестуванні цифрової стійкості, управлінні ризиками третіх сторін та обміні інформацією про загрози. Дана робота наголошує на необхідності для фінансових установ розробити комплексний підхід для досягнення відповідності DORA, що включає точне визначення та пом’якшення ІКТ-ризиків, стандартизацію звітності про інциденти, періодичне тестування систем та ретельний контроль сторонніх постачальників ІКТ-послуг. Це дослідження підкреслює, що дотримання цих принципів є критичним для посилення загальної стійкості фінансової системи.

Стаття [3] досліджує питання відповідності вимогам DORA, акцентуючи на конкретних вимогах до розробки програмного забезпечення для організацій фінансового сектору. Вона аналізує, як компанії, що надають фінансові послуги, повинні адаптувати свої процеси створення програмних продуктів, включаючи інтеграцію практик безпечної розробки (Secure SDLC) та управління ІКТ-ризиками, для задоволення стандартів, встановлених DORA. Дана робота є важливою для розуміння практичних аспектів

впровадження DORA, зокрема щодо забезпечення стійкості та безпеки програмного забезпечення у фінансових установах.

Метою статті є дослідження впливу регламенту DORA на процес безпечної розробки програмного забезпечення, визначення його критичних вимог до Secure SDLC, а також розробка рекомендацій щодо практичної інтеграції норм DORA в інфраструктуру фінансових організацій з метою забезпечення цифрової операційної стійкості.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Безпечний життєвий цикл розробки

Безпечний життєвий цикл розробки програмного забезпечення (Secure SDLC) інтегрує методи безпеки на кожному етапі процесу розробки програмного забезпечення. Такий підхід гарантує, що міркування щодо безпеки розглядатимуться командами розбробки з самого початку проекту, а не після проведеного тестування на проникнення.

Проактивно усуваючи вразливості, безпечний життєвий цикл розробки зменшує ймовірність витрат на виправлення після розгортання. Заходи захисту включаються в кожну фазу циклу розробки наступним чином:

1. Планування та збір вимог. На цьому етапі необхідно встановити вимоги безпеки разом із функціональними вимогами, забезпечуючи відповідність нормативним актам (наприклад, GDPR, HIPAA) і політикам безпеки організації. Також, на даному етапі проводиться моделювання загроз та визначаються потенційні загрози безпеці, вектори атак і агенти загроз.

2. Дизайн. На етапі дизайну необхідно впровадити елементи керування та принципи безпеки (наприклад, принцип мінімальних привілеїв, поглиблений захист) в архітектуру системи. Також, потрібно провести перевірку дизайну, щоб переконатися, що всі компоненти що використовуватимуться системою є безпечними.

3. Реалізація (Кодування). На даному етапі потрібно дотримуватись стандартів безпечного кодування (наприклад, OWASP, SANS), щоб запобігти типовим вразливостям, таким як SQL ін’єкції, XSS атаки і переповнення буфера. Для автоматизації виявлення вразливостей під час кодування може проводитись статичний аналіз коду, використовуючи інструменти для аналізу коду, для виявлення потенційних недоліків безпеки у вихідному коді під час його написання.

4. Тестування. На даному етапі виконуються різні типи тестування безпеки, зокрема: динамічне тестування безпеки програми (DAST) для виявлення вразливостей під час роботи програми, тестування на проникнення для імітації атак і виявлення слабких місць безпеки, та інтерактивне тестування безпеки додатків (IAST) використовуючи інструменти, які поєднують статичне та динамічне тестування в режимі реального часу, щоб виявити вразливості під час взаємодії програми з даними та користувачами.

5. Розгортання. На етапі розгортання відбувається зміцнення середовища з налаштуванням серверів, бази даних і мережевих компонентів відповідно до найкращих практик безпеки, щоб мінімізувати поверхню атаки. Також, даний етап гарантує безпечні та узгоджені конфігурації в різних середовищах (наприклад, розробка, тестування, продакшн), захищаючи конфіденційну інформацію, таку як ключі API та паролі. Для автоматизації, перевірки безпеки інтегруються в CI/CD, щоб кожен випуск проходив сканування безпеки та тестування перед тим, як досягти продакшн-середовища.

6. Технічне обслуговування та моніторинг. На даному етапі необхідно постійно відстежувати розгорнуте програмне забезпечення на наявність вразливостей, негайно застосовуючи виправлення та оновлення, проводити регулярні аудити безпеки, щоб перевірити цілісність програми та її середовища. Необхідно реалізувати надійні механізми журналювання та моніторингу для виявлення незвичних дій, можливих порушень і операційних проблем. Такі інструменти, як SIEM (Security Information and Event Management) — система управління інформацією та подіями безпеки, можуть допомогти шляхом кореляції журналів для виявлення аномалій.

7. Закінчення терміну експлуатації та виведення з експлуатації. Під час виведення з експлуатації потрібно переконатись, що дані безпечно видалено або заархівовано відповідно до політики організації та нормативних вимог. Також потрібно безпечно вивести з експлуатації будь-які компоненти, пов'язані з програмою, щоб запобігти несанкціонованому доступу або витоку даних.

Загалом, впровадження Secure SDLC мінімізує ризик порушення безпеки, зменшує витрати після розгортання, пов'язані з усуненням уразливостей, і забезпечує відповідність нормативним вимогам. Завдяки впровадженню безпеки на кожній фазі цей процес не лише захищає програму, але й сприяє підвищенню стійкості загальної архітектури програмного забезпечення.

Закон про цифрову операційну стійкість (DORA)

У час, коли фінансові інституції дедалі більше покладаються на цифрові технології, навіть короткочасний збій в IT-системі може мати серйозні наслідки. Втрати, викликані кібератаками, можуть сягати мільярдів євро, не кажучи вже про шкоду репутації. Саме тому Європейський Союз запровадив Digital Operational Resilience Act (DORA) — новий правовий інструмент, спрямований на зміцнення цифрової безпеки фінансового сектору. Європейський Союз (ЄС) посилює безпеку інформаційних технологій фінансових підприємств, таких як банки, страхові компанії та інвестиційні компанії, у відповідь на постійно зростаючі ризики, пов'язані з кібератаками. Закон про цифрову операційну стійкість (DORA) був попередньо схвалений Європейським парламентом 10 листопада 2022 року, а остаточне прийняття було досягнуто 28 листопада 2022. Компанії та організації, які працюють у фінансовому секторі, а також важливі треті сторони, які надають їм пов'язані з ІКТ послуги, такі як хмарні платформи або служби аналізу даних, зобов'язані відповідати стандартизованим вимогам безпеки DORA для своїх мереж та інформаційних систем, які розроблені для захисту від кібератак. DORA встановлює законодавчу базу щодо цифрової операційної стійкості, згідно з якою всі компанії, що охоплюють сферу дії, повинні гарантувати, що вони можуть протистояти, реагувати та відновлюватися після всіх видів збоїв і загроз, пов'язаних з ІКТ. Усі країни-члени ЄС мають однаковий набір правил, яких необхідно дотримуватися. Основною метою є запобігання та пом'якшення кіберзагроз [4].

У преамбулі регламенту визнається, що після фінансової кризи 2008 року вкрай необхідні реформи у фінансовому секторі посилили загальну стійкість галузі. Однак деякі аспекти безпеки ІКТ, такі як стійкість до цифрових атак, звітування про інциденти, пов'язані з ІКТ, і розгляд ІКТ як частини операційного ризику, не були повністю розглянуті.

Саме ці прогалини та збіги в існуючих правилах DORA прагне усунути та впорядкувати. DORA створила вичерпну, але комплексну структуру, яка гарантуватиме, що фінансові установи витримають, реагуватимуть і відновлюватимуться після збоїв, пов'язаних з ІКТ [5].

5 основних принципів DORA

Щоб забезпечити високий рівень цифрової операційної стійкості, Регламент DORA визначає низку ключових принципів, які мають стати основою для побудови безпечної та надійної ІКТ-інфраструктури у фінансовому секторі. Ці принципи охоплюють усі основні аспекти управління цифровими ризиками — від ідентифікації загроз до обміну розвідданими про кіберінциденти. Нижче наведено п'ять основних принципів, на яких базується підхід DORA до цифрової безпеки та стійкості:

1. **Управління ризиками ІКТ.** Управління ризиками є наріжним каменем мандата DORA. Розділ II Закону про цифрову операційну стійкість, а також його 12 розділів повністю присвячені управлінню ризиками ІКТ. Ця складова підкреслює необхідність для фінансових установ точно визначати, оцінювати та пом'якшувати ризики, пов'язані з ІКТ. Підприємства, які підпорядковуються DORA, повинні мати надійні інфраструктури для постійного моніторингу ключових цифрових систем, даних і з'єднань.
2. **Повідомлення про інциденти, пов'язані з ІКТ.** Повідомлення про інциденти та належне реагування на кіберінциденти є основою відповідності DORA. Цей розділ робить сильний акцент на стандартизації процесу звітування про інциденти у фінансовому секторі Європейського Союзу. Розділ III під назвою «Управління інцидентами, пов'язаними з ІКТ, класифікація та звітність» детально присвячено цьому принципу.

Згідно DORA, фінансові установи зобов'язані впроваджувати системи управління, які дозволяють їм відстежувати, описувати та повідомляти відповідним органам про будь-які значні інциденти, пов'язані з ІКТ. Таким чином DORA прагне підвищити здатність фінансового сектора реагувати на кіберзагрози та збої в роботі, та відновлюватися після них. Зрештою, це має на меті посилити загальну стійкість фінансової системи.

Важливо зазначити, що структура звітності повинна включати як внутрішні, так і зовнішні механізми звітності. Внутрішнє звітування означає швидке виявлення інцидентів і повідомлення про них усім важливим внутрішнім зацікавленим сторонам. Потім необхідно оцінити їхній вплив і вжити заходів для пом'якшення збитків. Зовнішнє звітування про інциденти стосується сповіщення регуляторних органів у разі руйнівного інциденту. У таких випадках, як порушення даних, це також може стосуватися постраждалих клієнтів, яких необхідно повідомити, якщо їхню конфіденційну фінансову інформацію було зламано.

3. **Тестування цифрової операційної стійкості.** DORA наполягає на тому, щоб фінансові установи періодично перевіряли свої системи управління ризиками ІКТ шляхом тестування цифрової операційної стійкості. Ці тести включають настільне тестування на основі сценаріїв, оцінку вразливостей, аналіз відкритого коду, тестування продуктивності, та тестування на проникнення на основі загроз тощо [6].

Цей принцип також наголошує на необхідності усунення прогалин, які випливають із результатів тестування. Виконання рекомендацій і заходів із виправлення також має бути перевірено, а їхня ефективність продемонстрована. Глава IV остаточного тексту DORA присвячена темі цифрового тестування операційної стійкості.

4. **Управління ризиками третіх сторін.** Глава V DORA та її два розділи охоплюють компонент «Управління ризиками третіх сторін у сфері ІКТ». Цей компонент вимагає від фінансових організацій ретельного проведення належної перевірки третіх сторін у сфері ІКТ. Мета полягає в тому, щоб гарантувати, що ці треті сторони дотримуються тих самих стандартів безпеки та стійкості, що й самі фінансові установи.

DORA вимагає, щоб контракти зі сторонніми постачальниками ІКТ включали певні обов'язкові положення для забезпечення дотримання цими постачальниками стандартів ЄС щодо управління ризиками та операційної стійкості. Контракти повинні періодично

переглядатися для забезпечення найвищих стандартів моніторингу. Очікується, що фінансові установи також документуватимуть будь-які ризики, що спостерігаються у їхніх сторонніх постачальників ІКТ. Важливо, що DORA підкреслює необхідність для фінансових організацій впроваджувати стратегію управління ризиками, пов'язаними зі сторонніми постачальниками ІКТ.

Цей компонент є надзвичайно важливим з огляду на зростаючу залежність фінансового сектору від зовнішніх ІКТ-послуг, особливо хмарних сервісів.

5. Обмін інформацією та розвідданими. Цей принцип, охоплений Розділом VI, сприяє обміну інформацією та розвідкою про загрози серед фінансової спільноти ЄС.

Середовище співпраці приносить користь усій галузі. Це найпростіший спосіб об'єднати зусилля проти просунутих кіберзагроз та бути на крок попереду. Оскільки організації в одній галузі створюють колективний пул знань, існує більша ймовірність передбачити кіберризики та бути готовими до боротьби з ними.

Обмін інформацією також може призвести до покращення цифрових практик стійкості до операцій і реалізації профілактичних заходів для боротьби з руйнівними подіями. Зрештою, це призводить до більш стабільної, надійної та безпечної фінансової інфраструктури в ЄС та за його межами.

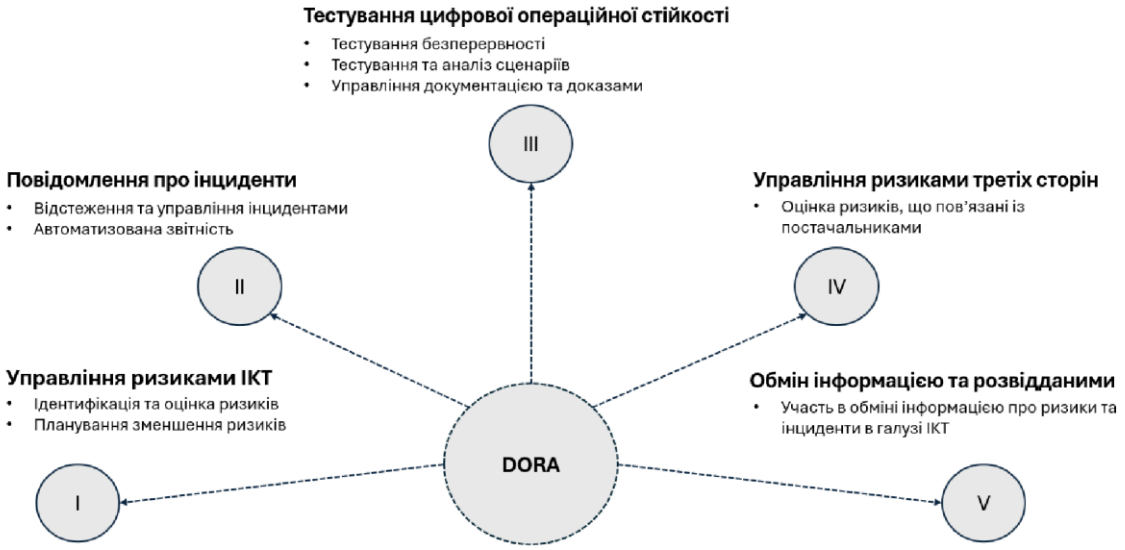

Рис 1. 5 основних принципів DORA

Аналіз вимог Digital Operational Resilience Act (DORA) до процесу розробки програмного забезпечення

DORA підкреслює важливість управління ризиками інформаційно-комунікаційних технологій (ІКТ) та забезпечення того, щоб організації могли протистояти, реагувати та відновлюватися після різних збоїв, включаючи кіберзагрози.

Ключові вимоги до процесу розробки програмного забезпечення в рамках DORA:

1. Управління ризиками ІКТ: Організації повинні розробити та впровадити комплексні системи управління ризиками в сфері ІКТ, які включають структури управління з наглядом на рівні ради директорів. Це передбачає проведення регулярних оцінок ризиків та інтеграцію протоколів кібербезпеки в процес розробки. Організації

повинні здійснювати постійний моніторинг ІКТ-ризиків, щоб адаптуватися до нових загроз, забезпечуючи безпеку свого програмного забезпечення протягом тривалого часу.

2. Безпечний життєвий цикл розробки програмного забезпечення (SDLC): Наголошуючи на проактивному підході до безпеки, розробники повинні враховувати міркування безпеки на ранніх стадіях процесу розробки, щоб мінімізувати ризики. Безпека має бути інтегрована на кожному етапі SDLC, від проектування до розгортання. Це передбачає застосування безпечних практик кодування [7], сканування вразливостей та використання перевірених бібліотек з відкритим кодом. Програмні системи повинні проходити ретельне тестування операційної стійкості, включаючи тести на проникнення і стрес-тести, щоб переконатися, що вони можуть протистояти збоям.

3. Тестування та оцінка цифрової операційної стійкості: Безперервне тестування є життєво важливим для підтримки стійкості фінансових програмних систем. Воно повинно включати тестування на проникнення, оцінку вразливостей, а також планування аварійних ситуацій і відновлення бізнесу. Усі заходи з тестування повинні бути ретельно задокументовані, з детальним описом використаних методологій, отриманих результатів та вжитих заходів для забезпечення дотримання стандартів DORA.

4. Управління інцидентами та звітність: Організації повинні мати чіткі плани управління інцидентами, які визначають механізми реагування на цифрові інциденти [8]. Це включає своєчасне інформування регуляторних органів про значні інциденти, пов'язані з ІКТ, у визначені терміни. Необхідно запровадити культуру постійного вдосконалення, в якій уроки, отримані з інцидентів, інтегруються в майбутні практики для підвищення стійкості

5. Управління ризиками, пов'язаними із постачальниками: Команди розробників повинні оцінювати стан безпеки сторонніх програмних компонентів і послуг, що використовуються в їхніх додатках. Контракти з постачальниками повинні включати положення про дотримання стандартів DORA, в тому числі вимоги щодо звітування про інциденти та управління ризиками [8].

Забезпечення вимог DORA під час розробки програмного забезпечення

Закон про цифрову операційну стійкість (DORA) підкреслює важливість життєвого циклу розробки програмного забезпечення (SDLC) як основи для забезпечення операційної стійкості фінансових установ. Забезпечуючи контроль на всіх етапах розробки, DORA сприяє дотриманню високих стандартів кібербезпеки та управління ризиками у фінтех-секторі. У табл. 1 наведено, як SDLC узгоджується з основними вимогами DORA:

Таблиця 1

Узгодження вимог DORA із SDLC

Вимога DORA	Стаття	Короткий опис вимоги	Узгодження із SDLC
Комплексна структура управління ризиками ІТ	Стаття 4	Впровадження системи управління ІТ-ризиками, що охоплює політики, процедури та нагляд	SDLC інтегрує оцінку ризиків на кожному етапі, що дозволяє системно виявляти й усувати вразливості та відповідати вимогам DORA
Повідомлення про інциденти	Стаття 17	Повідомлення про значні інциденти ІКТ до національних компетентних органів протягом 24 годин	Інтеграція моніторингу в реальному часі та автоматизованого виявлення інцидентів у SDLC сприяє своєчасному звітуванню згідно DORA

Тестування та стійкість	Стаття 19	Обов'язкове тестування на проникнення та тестування на основі загроз (TLPT) для об'єктів високого ризику	Етап тестування в SDLC дозволяє провести глибоку оцінку стійкості, що допомагає дотримуватись вимог DORA
Управління ризиками третіх сторін	Стаття 24	Контроль сторонніх постачальників ІКТ-послуг для забезпечення відповідності стандартам стійкості	Включення перевірки сторонніх учасників у SDLC допомагає пом'якшити ризики та виконати вимоги DORA
Обмін інформацією та співпраця	Стаття 28	Заохочення добровільного обміну даними про кіберзагрози для посилення колективної стійкості	Інтеграція безпечного обміну інформацією в SDLC підтримує спільну кіберстійкість відповідно до DORA

Регламент DORA приділяє значну увагу інтеграції вимог кібербезпеки безпосередньо у процеси створення, тестування та впровадження ІКТ-рішень. Це дозволяє мінімізувати ризики ще до появи продукту в експлуатаційному середовищі, забезпечуючи захищеність критичних сервісів фінансового сектору від потенційних загроз. Далі розглянемо основні підходи та механізми реалізації вимог DORA на всіх етапах життєвого циклу розробки програмного забезпечення:

1. Управління ризиками постачальників. У контексті регламенту DORA особливе значення надається контролю ризиків, пов'язаних із залученням зовнішніх ІКТ-постачальників, відкритого програмного забезпечення та хмарних сервісів. Через високу інтегрованість таких компонентів у сучасні ІТ-системи, забезпечення кіберстійкості неможливе без належного управління ланцюгами постачання [9].

Центральним інструментом такого підходу є ведення Software Bill of Materials (SBOM) — структурованого реєстру усіх компонентів ПЗ, що забезпечує прозорість та дозволяє ідентифікувати потенційно вразливі чи застарілі елементи. Поряд із цим, організації мають впроваджувати регулярну оцінку вразливостей сторонніх бібліотек і API з використанням SCA-інструментів, що інтегруються у CI/CD-процеси, та дозволяють оперативно виявляти ризики безпеки.

Ключовим аспектом є також контроль відповідності постачальників — укладення контрактів, які містять вимоги щодо безпеки, інцидент-менеджменту, аудиту та доступності. DORA покладає відповідальність за кіберстійкість не лише на постачальника, але й на організацію, що використовує послугу, вимагаючи прозорого та регулярного моніторингу її відповідність вимогам цифрової стійкості.

Загалом, управління ризиками постачальників в рамках DORA є багаторівневим процесом, який інтегрується у всі етапи життєвого циклу розробки програмного забезпечення та стає невід'ємною складовою цифрової безпеки фінансового сектору.

2. Тестування безпеки та постійний моніторинг. Регламент DORA накладає зобов'язання на організації фінансового сектору щодо впровадження системного підходу до безперервного тестування кібербезпеки та цілодобового моніторингу ІКТ-інфраструктури. Такий підхід відображає сучасну парадигму кіберстійкості, де безпека не може розглядатися як одноразовий етап чи аудит, а має стати динамічним, циклічним процесом, інтегрованим у всі фази розробки та експлуатації програмного забезпечення [9].

Однією з основних вимог DORA є впровадження автоматизованого тестування безпеки шляхом інтеграції інструментів типу SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing) та IAST (Interactive Application Security Testing) у CI/CD-процеси [10]. Це забезпечує раннє виявлення дефектів, підвищує якість коду та мінімізує ризики на етапі розгортання.

Паралельно з цим, регламент передбачає проведення регулярного тестування на проникнення, що дозволяє оцінити ефективність реалізованих заходів захисту, перевірити здатність ІТ-систем протистояти цілеспрямованим атакам і виявити нові вектори загроз, які не фіксуються традиційними сканерами.

Важливим компонентом стала також реалізація журналювання та моніторингу, що охоплює використання таких інструментів, як SIEM-системи для централізованого збору та кореляції логів, IDS/IPS-рішень для виявлення та блокування вторгнень, а також технологій поведінкового аналізу (UEBA) для ідентифікації аномальної активності, що може вказувати на приховані загрози [11]. Ці засоби забезпечують не лише оперативне реагування, але й створення цифрових слідів, необхідних для постінцидентного аналізу та підвищення стійкості систем у майбутньому.

Таким чином, безперервне тестування безпеки та постійний моніторинг, які вимагає DORA, трансформуються з технічного завдання у стратегічну функцію управління ризиками, яка визначає здатність фінансових установ функціонувати в умовах постійного зростання кіберзагроз.

3. Реагування на інциденти та забезпечення кіберстійкості в рамках DORA

Однією з ключових вимог регламенту DORA є впровадження ефективної та всеосяжної системи реагування на інциденти, що має гарантувати стабільність функціонування фінансових організацій навіть у разі реалізації кіберзагроз. У цьому контексті кіберстійкість розглядається не лише як здатність запобігати атакам, а й як можливість швидко виявити інцидент, локалізувати його наслідки та відновити нормальну діяльність без істотних втрат.

Важливу роль у цьому процесі відіграє автоматизоване виявлення загроз, що реалізується через системи поведінкового аналізу, які дозволяють виявляти нетипову активність у реальному часі. Використання таких рішень, як UEBA (User and Entity Behavior Analytics), дає змогу ідентифікувати загрози на основі відхилень від звичних шаблонів поведінки, що є особливо ефективним при боротьбі з новими, ще не класифікованими типами атак [12].

Не менш важливою складовою є регламентована звітність про інциденти, яку організації зобов’язані здійснювати відповідно до чітко визначених термінів та форматів, встановлених нормативною базою DORA. Це сприяє централізованому збору даних про кіберзагрози на рівні ЄС, формуванню превентивних заходів та вдосконаленню колективного реагування на інциденти в межах фінансового сектору.

Крім того, організації мають забезпечити оперативне відновлення після збоїв, що включає розробку та тестування стратегій резервного копіювання, впровадження механізмів обходу критичних точок відмови, а також забезпечення високої доступності сервісів у режимі 24/7. Відповідно до DORA, такі заходи мають бути невід’ємною частиною плану забезпечення безперервності бізнесу (BCP) та плану реагування на інциденти (IRP).

Таким чином, реагування на інциденти та забезпечення кіберстійкості в межах DORA формують структурований підхід до захисту цифрової інфраструктури, в якому технічні, організаційні та регуляторні компоненти взаємодіють задля забезпечення максимальної стійкості фінансових установ до деструктивного впливу кіберзагроз.

4. Підтримка безпеки після розгортання як ключовий елемент виконання вимог DORA. У післярелізному етапі життєвого циклу програмного забезпечення DORA вимагає від фінансових установ забезпечення стабільної кіберстійкості за умов динамічно змінюваного середовища загроз. Постійна підтримка безпеки після розгортання не є

допоміжною функцією, а становить невід'ємну частину стратегії цифрового захисту, що безпосередньо впливає на здатність установи адаптуватися до нових викликів.

Насамперед критичне значення має керування оновленнями, яке повинно здійснюватися відповідно до принципів безпечного випуску патчів. Це включає не лише оперативне усунення вразливостей, але й застосування перевірених механізмів доставки оновлень з обов'язковим тестуванням на предмет сумісності та відсутності нових ризиків. Регламент DORA передбачає інтеграцію цього процесу у загальну систему управління ризиками та безперервного вдосконалення ІКТ-інфраструктури.

Ще одним важливим елементом є навчання персоналу, оскільки навіть найнадійніші технічні засоби втрачають ефективність у разі низького рівня обізнаності працівників. Регулярне проведення тренінгів з кібербезпеки, імітація фішингових атак та моделювання інцидентів дозволяють підвищити загальну культуру безпеки в організації та мінімізувати вплив людського фактору.

Крім того, DORA підкреслює значення адаптивної безпеки, що реалізується шляхом інтеграції систем поведінкового аналізу та розвідки загроз (threat intelligence) у післярозгортальні процеси. Такі підходи дозволяють формувати гнучкі захисні механізми, здатні реагувати на нові типи атак та аномальні шаблони активності у реальному часі, зберігаючи при цьому ефективність протягом усього життєвого циклу ПЗ.

Загалом, підтримка безпеки після розгортання в контексті DORA перестає бути суто технічним завданням і трансформується у безперервний процес забезпечення кіберстійкості, що охоплює як технологічні, так і організаційно-поведінкові аспекти функціонування фінансової установи.

ВИСНОВКИ

Закон про цифрову операційну стійкість (Digital Operational Resilience Act, DORA) запроваджує нормативну базу, яка змінює життєвий цикл безпечної розробки програмного забезпечення (SDLC), акцентуючи увагу на кібербезпеці, управлінні ризиками та операційній стійкості. У цьому дослідженні проаналізовано вплив DORA на безпечну розробку фінансового програмного забезпечення, підкреслено його роль у зміцненні кіберстійкості, управлінні ризиками третіх сторін, тестуванні безпеки, реагуванні на інциденти та дотриманні нормативних вимог.

Результати дослідження демонструють, що DORA вимагає від фінансових установ інтегрувати заходи з кібербезпеки на ранніх стадіях розробки програмного забезпечення. Запроваджуючи стандарти безпечного кодування, автоматизоване тестування безпеки та постійний моніторинг, DORA гарантує, що програмне забезпечення залишається стійким до нових кіберзагроз. Крім того, регламент запроваджує суворі вимоги до управління ризиками постачальників, закликаючи фінансові компанії оцінювати та зменшувати ризики, пов'язані зі сторонніми постачальниками ІКТ.

Основний висновок цього дослідження полягає в тому, що дотримання вимог DORA — це не просто регуляторне зобов'язання, а стратегічна необхідність для фінансових установ, які прагнуть підтримувати безперервність бізнесу та операційну стійкість у все більш цифровому середовищі. Організації повинні привести свої практики SDLC у відповідність до мандатів DORA, впроваджуючи методології Secure SDLC.

Хоча DORA забезпечує надійну нормативну базу, її успішна реалізація залежить від організаційної готовності, інвестицій в експертизу з кібербезпеки та постійної адаптації до нових загроз. Майбутні дослідження повинні вивчити практичні виклики

прийняття DORA та оцінити його довгострокову ефективність у зменшенні ризиків кібербезпеки у фінансових установах.

Впроваджуючи принципи DORA в безпечну розробку програмного забезпечення, організації можуть проактивно зміцнювати свою позицію з кібербезпеки, забезпечуючи відповідність вимогам, одночасно підвищуючи довіру та стабільність фінансового сектору перед обличчям нових цифрових загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554.* (n. d.). https://www.digital-operational-resilience-act.com/
2. *Preparing for DORA: 5 Pillars of DORA and How to Achieve Compliance.* (n. d.). https://sigma.software/about/media/preparing-for-dora-5-pillars-of-dora-and-how-to-achieve-complia nce
3. *Navigating DORA Compliance: Software Development Requirements for Financial Services Companies*. (n. d.). https://jfrog.com/blog/navigating-dora-compliance-software-development-requirements-for-financialservices-companies/
4. *Digital Operational Resilience Act (DORA) - Central Bank of Ireland.* (n. d.). https://www.centralbank.ie/regulation/digital-operational-resilience-act-dora
5. *What is DORA? - Microsoft Learn.* (n. d.). https://learn.microsoft.com/en-us/compliance/dora/dora-what-is-dora
6. *DORA Regulation: Summary, Compliance Checklist + Training – Hoxhunt.* (n. d.). https://hoxhunt.com/blog/dora-regulation
7. *Secure Software Development Lifecycle (SSDLC) - Security-as-a-Service.io.* (n. d.). https://security-as-a-service.io/en/it-security-solutions/secure-software-development-lifecycle-ssdlc-how-companies-integrate-security-into-the-development-process-with-iso-27001-and-c5/
8. *Third-Party Risk Management under DORA - SAP LeanIX.* (n. d.). https://www.leanix.net/en/wiki/trm/third-party-risk-management-under-dora
9. *Art. 6 ICT risk management framework - dora-info.eu.* (n. d.). https://www.dora-info.eu/dora/article-6/
10. *DORA: EU regulation on digital operational resilience of financial institutions – Deloitte.* (n. d.). https://www.deloitte.com/cz-sk/en/services/consulting/perspectives/eu-dora-digital-operational-resilience-act-fo r-financial-services.html
11. *Implementing DORA: EU Financial Entities, Here's What You Should Know – Sprinto.* (n. d.). https://sprinto.com/blog/dora-implementation/
12. *Reporting Major ICT-related Incidents and Significant Cyber Threats under DORA - Central Bank of Ireland.* (n. d.). https://www.centralbank.ie/regulation/digital-operational-resilience-act-dora/reporting-major-ict-related-inciden ts-and-significant-cyber-threats

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Yevhen Kurii
Doctor of Philosophy, Assistant Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-3423-5655
yevhenii.o.kurii@lpnu.ua

Vitalii Susukailo
Doctor of Philosophy, Assistant Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-4431-9964
vitalii.a.susukailo@lpnu.ua

Anna Yerofeieva
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0001-3256-1019
anna.yerofeieva.kb.2021@lpnu.ua

Marta Nesteriuk
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0006-4229-7019
marta.nesteriuk.kb.2021@lpnu.ua

ANALYSIS OF THE IMPACT OF DIGITAL OPERATIONAL RESILIENCE ACT (DORA) REQUIREMENTS ON THE PROCESS OF SECURE SOFTWARE DEVELOPMENT

Abstract. The article provides a comprehensive analysis of the impact of the European Union's Digital Operational Resilience Act (DORA) Regulation on the Secure Software Development Life Cycle (Secure SDLC) in the financial sector. In the context of the rapid digital transformation of banking, insurance and investment services, the DORA forms a new mandatory regulatory framework for digital operational resilience, covering a wide range of areas, including information and communication technology (ICT) risk management, mandatory reporting of serious cyber incidents, regular security testing, control of IT service providers, and coordination of threat information exchange between financial market participants. The paper discusses in detail the five key DORA requirements defined in the text of the Regulation, with an emphasis on their consistent integration into all stages of the Secure SDLC - from initialization, planning, requirements analysis, and architecture design to implementation, testing, deployment, technical support, modernization, and decommissioning. Particular attention is paid to the implementation of automated security testing tools (SAST, DAST, IAST), the use of abnormal activity detection systems (SIEM, UEBA), the implementation of Software Bill of Materials (SBOM) to increase component transparency, as well as the development and implementation of incident response plans (IRP) and business continuity plans (BCP). A table of alignment of the key DORA articles with the relevant phases of the SDLC life cycle is proposed, which allows identifying critical compliance points, reducing security gaps and optimizing the implementation of digital resilience requirements. The study examines modern approaches to integrating security practices into CI/CD processes, the importance of raising employees' awareness of current cyber threats, and the formation of a security culture focused on proactive protection even after software deployment. It is noted that compliance with DORA requirements should not be viewed solely as a response to regulatory pressure, but as a basis for the long-term transformation of corporate digital security in financial institutions. The results of the study are of interest to software developers, information security professionals, risk management professionals, regulators, and internal and external auditors seeking to ensure compliance with new regulatory requirements and strengthen the digital resilience of organizations in a high-risk environment.

Keywords: DORA; Secure SDLC; cyberresilience; ICT risk management; financial institutions; monitoring; incident response.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554.* (n. d.). https://www.digital-operational-resilience-act.com/
2. *Preparing for DORA: 5 Pillars of DORA and How to Achieve Compliance.* (n. d.). https://sigma.software/about/media/preparing-for-dora-5-pillars-of-dora-and-how-to-achieve-complia nce
3. *Navigating DORA Compliance: Software Development Requirements for Financial Services Companies.* (n. d.). https://jfrog.com/blog/navigating-dora-compliance-software-development-requirements-for-financialservices-companies/
4. *Digital Operational Resilience Act (DORA) - Central Bank of Ireland.* (n. d.). https://www.centralbank.ie/regulation/digital-operational-resilience-act-dora
5. *What is DORA? - Microsoft Learn.* (n. d.). https://learn.microsoft.com/en-us/compliance/dora/dora-what-is-dora
6. *DORA Regulation: Summary, Compliance Checklist + Training – Hoxhunt.* (n. d.). https://hoxhunt.com/blog/dora-regulation
7. *Secure Software Development Lifecycle (SSDLC) - Security-as-a-Service.io.* (n. d.). https://security-as-a-service.io/en/it-security-solutions/secure-software-development-lifecycle-ssdlc-how-companies-integrate-security-into-the-development-process-with-iso-27001-and-c5/
8. *Third-Party Risk Management under DORA - SAP LeanIX.* (n. d.). https://www.leanix.net/en/wiki/trm/third-party-risk-management-under-dora
9. *Art. 6 ICT risk management framework - dora-info.eu.* (n. d.). https://www.dora-info.eu/dora/article-6/
10. *DORA: EU regulation on digital operational resilience of financial institutions – Deloitte.* (n. d.). https://www.deloitte.com/cz-sk/en/services/consulting/perspectives/eu-dora-digital-operational-resilience-act-fo r-financial-services.html
11. *Implementing DORA: EU Financial Entities, Here's What You Should Know – Sprinto.* (n. d.). https://sprinto.com/blog/dora-implementation/
12. *Reporting Major ICT-related Incidents and Significant Cyber Threats under DORA - Central Bank of Ireland.* (n. d.). https://www.centralbank.ie/regulation/digital-operational-resilience-act-dora/reporting-major-ict-related-inciden ts-and-significant-cyber-threats