

УДК 004.056.5

**О. Лавринець, І. Грод**

Тернопільський національний технічний університет імені Івана Пулюя

## **ПОБУДОВА СЕРЕДИ РОЗРОБКИ ВЕБ-ДОДАТКІВ З ОПТИМАЛЬНИМ РІВНЕМ БЕЗПЕКИ**

UDC 004.056.5

**O. Lavrynets, I. Grod**

(Ternopil Ivan Pului National Technical University, Ukraine)

## **BUILDING A WEB APPLICATION DEVELOPMENT ENVIRONMENT WITH OPTIMAL SECURITY**

Досягнення в області веб-технологій в поєднанні зі змінною бізнес-середовищем означають, що веб-додатки стають все більш поширеними в корпоративній, державній та урядовій сферах послуг.

Хоча веб-додатки можуть забезпечити зручність і ефективність в сфері послуг, також вони представляють ряд нових загроз безпеці, які потенційно можуть становити значні ризики для інфраструктури інформаційних технологій організації, якщо її не обробляти належним чином.

В даний час на ринку переважають гнучкі методології розробки – Agile. Рівень виконання вимог безпеки вкрай залежний від декількох факторів:

- досвідченість команди. Досвід в розробці захищених систем. Наявність Project Backlog.
- присутність в проекті фахівця з комп'ютерної безпеки.
- рівень зрілості компанії. Наявність корпоративних правил забезпечення безпеки в проектах.
- досвід підтримки веб-додатків

Інша проблема полягає в малій цінності вимог безпеки для замовника в порівнянні з продає функціональністю. Таким чином вимоги безпеки можуть бути відсунуті реалізацією продає функціональності. Це є однією з основних причин низького ступеня захищеності більшості сучасних веб-додатків.

Дослідження вразливостей веб-додатків, що проводяться компанією Positive Technologies в 2018 році показало, що загальний рівень захищеності веб-додатки продовжує знижуватися. Розробники прагнуть забезпечити максимальну функціональність систем і не завжди приділяють належну увагу безпеці коду. При цьому, наголошується широку поширеність недоліків, пов'язаних з помилками адміністрування.

Необхідно провести дослідження про вбудовуванні вимог безпеки в гнучку методологію розробки ПО. Знизити вплив досвіду компанії і команди розробників, а також існування в компанії процесів забезпечення безпеки веб-додатків. Це може бути досягнуто автоматизацією реалізації вимог безпеки. Проблема малої цінності вимог безпеки щодо функціональності може вирішитися зменшенням необхідного для впровадження вимог безпеки часу.

### **Література**

1. Positive Technologies – Уязвимости веб-приложений 2018 [Електронний ресурс] URL:<https://www.ptsecurity.com/ru-ru/research/analytics/web-application-vulnerabilities-statistics-2019/>
2. OWASP – Top Ten Proactive Controls [Електронний ресурс]// URL: [http://master.cmc.msu.ru/files/OWASP\\_Top\\_Ten\\_Proactive\\_Controls\\_v2\\_rus.pdf](http://master.cmc.msu.ru/files/OWASP_Top_Ten_Proactive_Controls_v2_rus.pdf)