УДК 004.41:004.056

КОВАЛЕНКО О. В., канд. техн. наук, доцент кафедри кібербезпеки та програмного забезпечення (Центральноукраїнський національний технічний університет)

# Методи та засоби управління безпекою додатків

*В роботі запропоновано ряд практичних рекомендацій з управління силами і засобами безпеки IT-організацій в умовах використання гнучких методологій розробки програмного забезпечення Agile. У загальному випадку такі корегування можуть реалізуватися в таких практичних напрямах: перегляд парадигми безпеки додатків; Розподіл команди; розширення повноважень експертів безпеки в процесі вдосконалення команди; постійний перегляд вимог, методів, засобів, алгоритмів та інших даних при управлінні безпекою. Перегляд парадигми безпеки додатків приводить до розуміння необхідності постійного збільшення частки автоматизованих підходів управління процесами на всіх етапах розробки і реалізації IT-продуктів та послуг. Розподіл команди дозволить забезпечити заданий рівень якості додатків без залучення значних ресурсів та сил (експертів). Розширення повноважень експертів безпеки в процесі вдосконалення команди дозволяє перевіряти організацію розробки, документів та питань безпеки, організацію роботи з ключовими елементами безпеки. Постійний перегляд вимог, методів, засобів, алгоритмів та інших даних при управлінні безпекою дозволяє проаналізувати і оцінити зміни в IT-системі, середовищі обробки, політиці безпеки.*

***Ключові слова:*** *управління безпекою додатків, Agile, розробка програмного забезпечення.*

**Постанова проблеми**

Проектне управління в сфері IT можна розглядати за допомогою вивчення ефективних підходів, методик і способів надання послуг. Всі розроблені методи управління проектами відрізняються деталізованістю, формалізованістю, галузями застосування та ін. Такі методи управління проектами є дуже різноманітними системними підходами до управління. Отже, як програмне забезпечення наявний ряд відмінних концепцій.

Більшість сучасних IT-фірм також схильна до постійної динамічної зміни, розширення та оновлення своїх компонентів, а їх продукція (програмні додатки) – оновлення новими версіями. Крім того, в процесі розробки відбуваються кадрові зміни, а з плином часу змінюється і політика безпеки. Ці зміни викликають нові ризики, а ризики, які раніше були передбачені, можуть знову стати проблемою. Таким чином, процес управління ризиками безпеки в IT-сфері знаходиться в постійному розвитку [1-6].

**Аналіз останніх досліджень і публікацій**

Аналіз літератури [1-8], а також проведені дослідження показали, що більшість існуючих методів та засобів управління безпекою в IT-сфері враховують можливості вже застарілої методології розробки – «Waterflow». Однак в даний час більшість фірм використовує гнучкі методології розробки й управління, засновані на філософії Agile. Це накладає деякі особливості (обмеження), описані в [1, 3], на методи і вимагає від керівників проектів внесення деяких корегувань у процес розробки та експлуатації.



У загальному випадку такі корегування можуть реалізуватися в наступних практичних напрямках.

1. Перегляд парадигми безпеки додатків.
2. Розподіл команди.
3. Розширення повноважень експертів безпеки в процесі вдосконалення команди.
4. Постійний перегляд вимог, методів, засобів, алгоритмів та інших даних при управлінні безпекою.

**Метою роботи** є визначення ряду практичних рекомендацій для використання методів та засобів управління безпекою додатків.

**Основна частина**

Розглянемо більш докладно кожен із зазначених напрямків.

У ранніх парадигмах безпеки додатків експерти звикли сприймати стан безпеки як щось особливе, окреме від усього додатку. Однак в сучасних умовах використання гнучких методологій філософії Agile безпека – це одна з властивостей якості додатків. IT-фірми шукають різні підходи в управлінні безпекою своїх продуктів. Наприклад, корпорація Microsoft надала своє бачення процесу безпечної розробки у вигляді схеми (рис. 1).

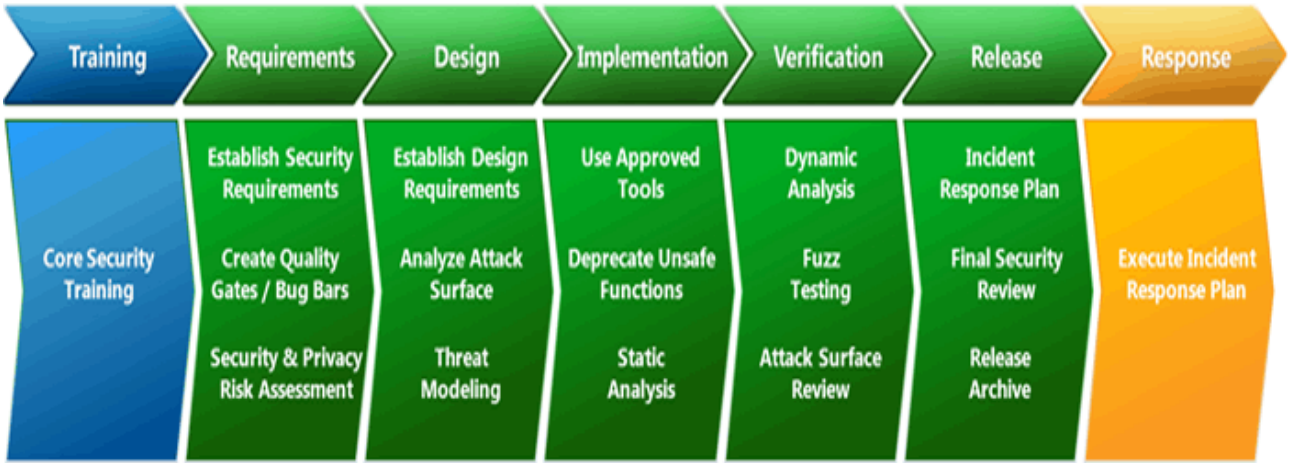


Рис. 1. Схема безпечної розробки програмного забезпечення відповідно до філософії Microsoft

У цих умовах дуже важливим стає розуміння необхідності постійного збільшення частки автоматизованих підходів управління процесами на всіх етапах розробки та реалізації ІТ-продуктів і послуг.

В умовах розробки та реалізації достатньо великих проектів (програм) існує необхідність (за можливості) використання множини різних команд (можливо, ще й розподілених), що виконують різні завдання. При цьому вимоги, можливості, методології розробки та інші практики у всіх різні. Не кажучи вже про навички «безпеки». На жаль, ІТ-фірми дуже рідко можуть собі дозволити мати експертів безпеки в кожній команді. У той же час вимоги максимально безпечної розробки, без застосування методу «одна команда – один експерт безпеки» залишаються. У цих умовах доцільно скористатися способом масштабування процесу розробки програмного забезпечення, що описаний в роботах [1-4]. Це дозволить забезпечити заданий рівень якості додатків без залучення значних ресурсів та сил (експертів).

Одною з основних переваг гнучких методологій розробки та управління ІТ-проектами є набуття та накопичення досвіду учасниками проектів. При цьому безпека продукту є питанням розробників, їх знань і контролю, а не окремих команд і людей, тому розширення відповідальності розробників, а також попередніх перевірок може бути доцільним.

Виходячи з цього в рамках існуючих заходів (наприклад, мітингу-ретроспективи), передбачених Agile, доцільно проводити додаткові тренінги, воркшопи, мініквести або інші заходи, основною метою яких є передача досвіду тестування експертами безпеки розробникам. Звичайно, необхідно враховувати нестачу часових ресурсів як з боку тих, хто навчається, так і з боку тих, хто навчає. Тому доцільно використовувати такі правила навчання:

1. Інтерактивні модулі навчання замість нудних слайдів або відео.
2. Приклади вразливостей з реального життя та пентестів.
3. Той, хто навчається, сам імітує дії атакуючого для розуміння суті атаки.
4. Пояснення помилок в коді для розробників.
5. Рекомендації з написання коду для розробників тією мовою програмування, яка потрібна.

Крім того, завжди є фінальне ревю, на якому команда перевіряє документацію, проводить тести безпеки та ін. При цьому експерти безпеки стають такою собі «організуючо-перевіряючою» ланкою, а також командою супроводу інших команд. Вони розробляють вимоги, інструкції та інструменти, дають рекомендації і проводять тренінги.

Дуже важлива при цьому комунікація експертів з командою. Це дозволяє перевіряти організацію розробки, документів та питань безпеки, організацію роботи з ключовими елементами безпеки. При цьому проводиться аналіз слабких місць команди на різних етапах і організовується зворотній зв’язок команді.

Проведені дослідження, а також аналіз літератури [4-8] показали, що процес оцінки ризику необхідно проводити з певною періодичністю. У ряді керівних документів ця періодичність обмежується одним разом на три роки. Однак управління ризиками проводиться не тому, що це потрібно законодавчим актом, а тому що це хороша практика підтримки бізнес-цілей організації.

У зв’язку з цим графік оцінки та зменшення ризиків, пов’язаних з безпекою, повинен бути достатньо гнучким, щоб можна було проаналізувати та оцінити зміни в ІТ-системі, середовищі обробки, політиці безпеки.

Відповідаючи на питання необхідності проведення тестування безпеки додатків, можна відзначити, що ряд експертів пропонує проводити тестування:

– для вже використовуваних критичних додатків – з вибраною періодичністю або при внесенні змін;

– перед запуском в експлуатацію нового бізнес-додатка;

– при додаванні компонентів до існуючих додатків;

– в разі інциденту інформаційної безпеки, пов'язаного з функціонуванням додатка і при підозрі на некоректну роботу додатка з точки зору інформаційної безпеки.

Також слід зазначити, що успішна програма управління ризиками неможлива без спільної підтримки та участі керівництва, команди та експертів безпеки.

**Висновки**

В роботі запропоновано ряд практичних рекомендацій з управління силами та засобами безпеки IT-організацій в умовах використання гнучких методологій розробки програмного забезпечення Agile. Виконання даних рекомендацій дозволяє: зрозуміти необхідність постійного збільшення частки автоматизованих підходів управління процесами на всіх етапах розробки та реалізації IT-продуктів і послуг; забезпечити заданий рівень якості додатків без залучення значних ресурсів та сил (експертів); перевіряти організацію розробки, документів та питань безпеки, організацію роботи з ключовими елементами безпеки; проаналізувати та оцінити зміни в IT-системі, середовищі обробки, політиці безпеки. Успішна програма управління ризиками неможлива без спільної підтримки та участі керівництва, команди та експертів безпеки.

**Література**


1. Ruby, S., Thomas, D. and Hansson, D.H. Agile Web Development with Rails 4 Pragmatic Programmers LLC [Text]. – 2013. – 439 p. ISBN: 978-1-93778-556-7.
2. Putu, Adi and Guna, Permana Scrum Method Implementation in a Software Development Project Managemen. International Journal of Advanced Computer Science and Applications [Text]. – 2015. – № 6 (9). – P. 199–205.
3. Махметов, Г. Е. Когда «Agile» (не) к месту [Электронный ресурс] / Г. Е. Махметов. – Режим доступа : https://makhmetov.ru/articles/agile.html.
4. Kruger Freddie, Ladikos Anastasios The development of a crime prevention model within a commercial production area.Tydskr. geesteswet [Text]. – 2008. – № 48 (4). – P. 439-453. ISSN 2224-7912.
5. Семенов, С. Г. Масштабирование гибкой методологии разработки программного обеспечения с учетом требований безопасности [Текст] / С. Г. Семенов, К. Халифе, В. Н. Змиевская // Методи та засоби кодування, захисту й ущільнення інформації : матеріали 6 Міжнар. наук.-практ. конф. – Вінниця : ВНТУ, 2017. – С. 81-83.
6. Семенов, С. Г. Усовершенствованный способ масштабирования гибкой методологии разработки программного обеспечения [Текст] / С. Г. Семенов, К. Халифе, М. М. Захарченко // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т. 1(1). – С. 79-84.
7. Применение метода двухфазной компиляции на основе LLVM для распространения приложений с использованием облачного хранилища. [Электронный ресурс] / С. С. Гайсарян [и др.] // Труды института системного программирования РАН. – 2014. – С. 315-326. Режим доступа : https://cyberleninka.ru/article/n/primenenie-metoda-dvuhfaznoy-kompilyatsii-na-osnove-llvm-dlya-rasprostraneniya-prilozheniy-s-ispolzovaniem-oblachnogo-hranilischa
8. Stoneburner G., Goguen A., Feringa A. Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology [Text]. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, 2002. – P. 55.



**Коваленко А. В. Методы и средства управления безопасностью приложений.** В работе предложен ряд практических рекомендаций по управлению силами и средствами безопасности IT-организаций в условиях использования гибких методологий разработки программного обеспечения Agile. В общем случае такие корректировки могут реализоваться в следующих практических направлениях: просмотр парадигмы безопасности приложений; распределение команды; расширение полномочий экспертов безопасности в процессе совершенствования команды; постоянный пересмотр требований, методов, средств, алгоритмов и других данных при управлении безопасностью. Просмотр парадигмы безопасности приложений приводит к пониманию необходимости постоянного увеличения доли автоматизированных подходов управления процессами на всех этапах разработки и реализации IT-продуктов и услуг. Распределение команды позволит обеспечить заданный уровень качества приложений без привлечения значительных ресурсов и сил (экспертов). Расширение полномочий экспертов безопасности в процессе совершенствования команды позволяет проверять организацию разработки, документов и вопросов безопасности, организацию работы с ключевыми элементами безопасности. Постоянный

пересмотр требований, методов, средств, алгоритмов и других данных при управлении безопасностью позволяет проанализировать и оценить изменения в IT-системе, среде обработки, политике безопасности.
**Ключевые слова:** управление безопасностью приложений, Agile, разработка программного обеспечения.

***Коваленко Олександр Володимирович***, *кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.*
*E-mail: clashav@gmail.com; ORCID ID: https://orcid.org/0000-0001-9297-0650* .

---

**Kovalenko O. Methods and means for security management of applications.** The purpose of the work is to identify a number of practical recommendations for using methods and tools for managing application security. The paper proposes a series of practical recommendations on the management of the forces and means of security of IT organizations in the context of the use of flexible methodologies for the development of software Agile. In the general case, such adjustments can be realized in the following practical directions: Viewing the application security paradigm; Distribution of the team; Expand the powers of security experts in the process of team improvement; Constant review of requirements, methods, tools, algorithms and other data in security management. The implementation of these recommendations allows: to understand the need for a constant increase in the share of automated process management approaches at all stages of the development and implementation of IT products and services; to provide the given level of quality of applications without involving significant resources and forces (experts); check organization of development, documents and safety issues, organization of work with key security elements; analyze and evaluate changes in the IT system, processing environment, security policy. A successful risk management program is not possible without joint support and involvement of management, team and security experts.
**Keywords:** application security management, Agile, software development.

***Kovalenko Oleksandr,*** *Candidate of Engineering Sciences, Associate Professor of Cybersecurity & Software Academic Department Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.*
*E-mail: clashav@gmail.com; ORCID ID: https://orcid.org/0000-0001-9297-0650* .

*Надійшла 06.06.2018 р.*