УДК 004

Е. А. Малышев[1]*

Обеспечение информационной безопасности технологического конвейера разработки программного обеспечения

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: egormalyshev2001@gmail.com

Аннотация. В работе рассматривается жизненный цикл программных и аппаратно-программных проектов, исследуется и систематизируется проблематика обеспечения локальной и сетевой информационной безопасности процессов на каждом этапе: от стадии планирования до тестирования и эксплуатации созданного продукта. На обзор выносится один из возможных подходов к обеспечению комплексной информационной безопасности инфраструктуры технологического конвейера разработки программных и аппаратно-программных решений. Данный подход разработан в соответствии с комплексными методологиями DevOps и DevSecOps. В результате работы был получен программный модуль, обеспечивающий комплексную информационную безопасность корпоративной инфраструктуры в части технологического конвейера разработки программных решений за счет использования многослойной изоляции программного обеспечения, имплементации системы обнаружения и предотвращения событий, а также обеспечения непрерывного мониторинга инфраструктуры.

Ключевые слова: DevOps, DevSecOps, CI/CD, IDS/IPS, SIEM, DLP, VPN

E. A. Malyshev[1]*

Ensuring information security of the software development technology pipeline

[1] National Research Nuclear University "MEPhI", Moscow, Russian Federation
* e-mail: egormalyshev2001@gmail.com

Abstract. The paper considers the life cycle of software and hardware-software projects, investigates and systematizes the issues of ensuring local and network information security of processes at each stage, from planning to testing and operation of the created product. One of the possible approaches to ensuring comprehensive information security of the infrastructure of the technological conveyor for developing software and hardware-software solutions is presented. This approach was developed in accordance with the comprehensive DevOps and DevSecOps methodologies. The work resulted in a software module that provides comprehensive information security of corporate infrastructure in terms of the technological pipeline of software solutions development through the use of multi-layer software isolation, implementation of event detection and prevention system, as well as ensuring continuous monitoring of the infrastructure.

Keywords: DevOps, DevSecOps, CI/CD, IDS/IPS, SIEM, DLP, VPN

Введение

Развитие методологий построения процессов внутри команд по разработке программного обеспечения привело к появлению комплексной методологии *DevOps,* являющейся набором практик, объединяющих разработку программ-

ного обеспечения (англ. *Development*), и его эксплуатацию (англ. *Operations*) и направленных на сокращение жизненного цикла разработки, а также обеспечение непрерывной поставки программного обеспечения.

Одной из ключевых методик, входящих в DevOps, является построение работоспособного конвейера непрерывной интеграции и непрерывной доставки (англ. *CI/CD pipeline, Continuous Integration/Continuous Delivery*). Основными принципами, в соответствии с которыми проектируются автоматизированные конвейеры разработки программного и аппаратно-программного обеспечения, являются разделение ответственности, снижение рисков и сокращение цикла обратной связи [1]. Исследования ученых *F.M.A. Erich, C. Amrit* и *M. Daneva,* в свою очередь, доказывают эффективность внедрения методологии *DevOps* на практике в реальных командах разработки [2]. В то же время качественные показатели, демонстрирующие успешность применения практик *DevOps*, представлены научной школой *Michael Hilton* [3]. В ряде работ в первую очередь рассматриваются оптимизация и ускорение процессов жизненного цикла программного обеспечения и упускается часть по обеспечению информационной безопасности процессов конвейера.

На фоне увеличения активности со стороны злоумышленников возрастает потребность в обеспечении надежности и отказоустойчивости информационно-вычислительной инфраструктуры предприятия в целом и защищенности технологического конвейера разработки программного и/или аппаратно-программного обеспечения в частности, поскольку отказ в работе инструментария, задействованного в ходе разработки программного обеспечения, привносит значительные издержки предприятию-разработчику программных решений.

Использование различных решений, таких как система обнаружения вторжений, система непрерывного мониторинга, а также системы идентификации и корреляции событий позволяет улучшить комплексную защищенность информационного периметра предприятия [4-6]. Конвергенция данных технологий с использованием виртуальных частных сетей позволяет добиться значительного уровня безопасности сети предприятия [7].

Соответственно, возрастает актуальность разработки подходов к обеспечению информационной безопасности прикладного программного обеспечения, реализующего непрерывную работу технологического конвейера предприятия.

Постановка задачи и цель исследования

Целью работы является проектирование и реализация метода обеспечения качества, надежности, отказоустойчивости и безопасности приложений с использованием автоматизированных средств осуществления проверок, а также применения многослойной изоляции программного обеспечения с использованием систем контейнеризации и виртуализации прикладного программного обеспечения.

Разбиение общей цели на задачи было выполнено с применением методов системного анализа и декомпозиции общей цели. В ходе проведения исследовательской работы был выделен ряд задач:

– исследование предметной области;
– постановка задачи;
– моделирование предметной области при помощи диаграмм;
– планирование и проектирование автоматизированного конвейера разработки программных компонентов;
– программная реализация автоматизированного конвейера разработки программных компонентов;
– проведение автоматизированного тестирования разработанного решения.

Предлагаемое решение

Достижение поставленной цели сопровождается разработкой метода, проектированием на его основе технологического конвейера разработки программного и аппаратно-программного обеспечения, а также разработкой конечного решения, автоматизирующего процессы развертки и конфигурирования выбранного программного стека.

Выбор конкретного программного стека обуславливается требованиями со стороны бизнеса и регуляторов, опытностью команды разработки и эксплуатации, а также совместимостью с уже имеющимся программным обеспечением. Ошибочный выбор прикладного программного обеспечения, не отвечающего всем требованиям, в свою очередь может привести к дополнительным издержкам со стороны хозяйствующего субъекта.

Метод сопровождения технологических процессов конвейера приведен на рис. 1.

Обеспечение информационной безопасности программного продукта в рамках каждого из этапов, представленных на рис. 1, является ключевой задачей. Для этих целей предлагается использование следующего прикладного программного обеспечения (рис. 2).

Каждый из компонентов конвейера предлагается разворачивать в отдельных *docker*-контейнерах на различных виртуальных машинах, что способствует повышению уровня безопасности информационных потоков конвейера за счет изоляции процессов, достигаемой многослойной инкапсуляцией с применением средств виртуализации и контейнеризации [8].

Помимо использования средств изоляции программного обеспечения предлагается внедрение виртуальной частной сети (от англ. *VPN*). Данное решение позволит обеспечить защищенное соединение между клиентом и сервером посредством внесения дополнительного слоя шифрования, защищающего данные от несанкционированного доступа. *UML*-диаграмма на рис. 2 демонстрирует схему взаимодействия компонентов при использовании распределенной архитектуры. В случае развертки данного решения локально архитектура программного комплекса подлежит адаптации для уменьшения издержек скорости пересылки данных между компонентами приложения.

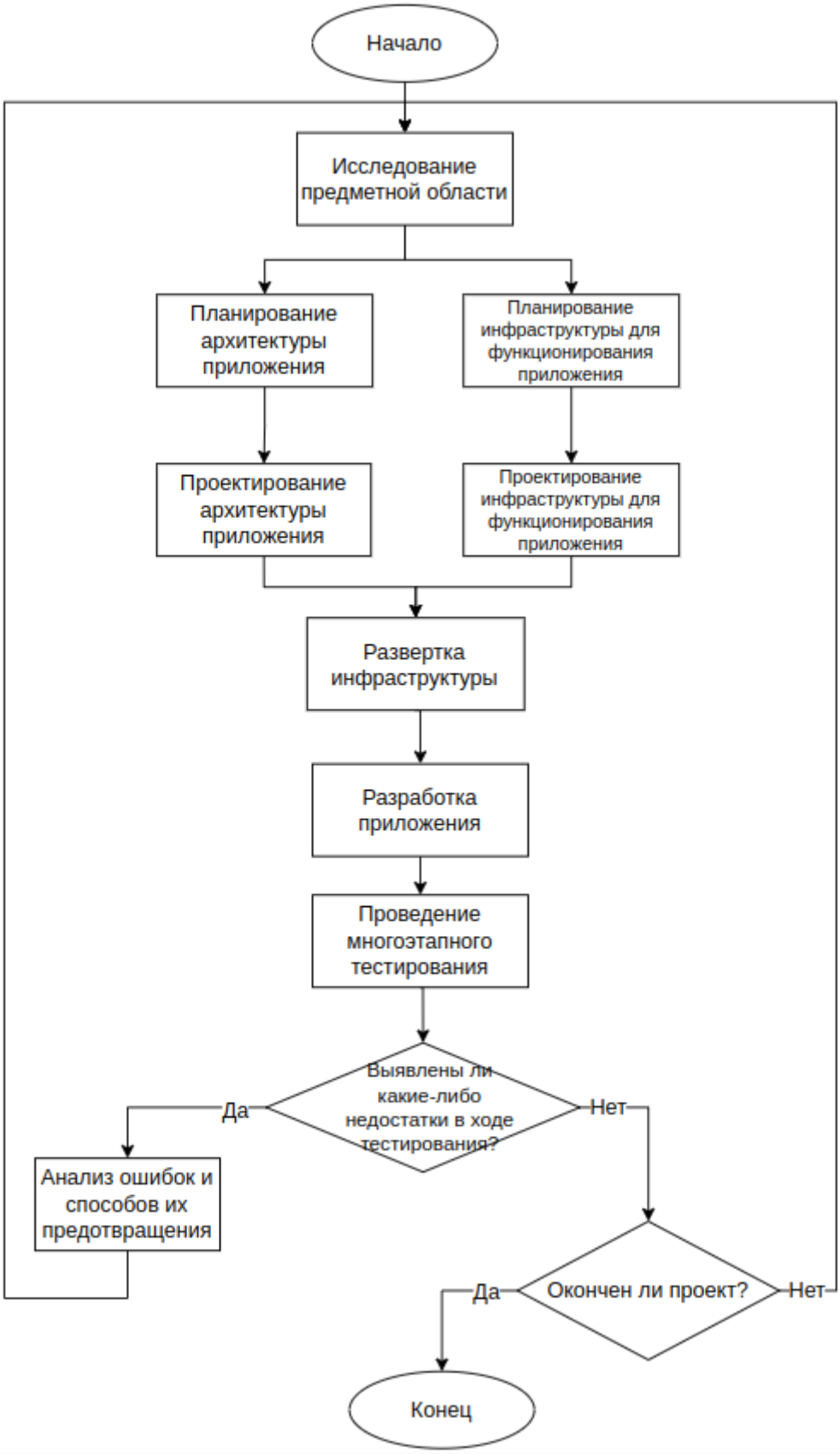

Рис. 1. Блок-схема метода сопровождения технологического конвейера разработки программных и аппаратно-программных решений

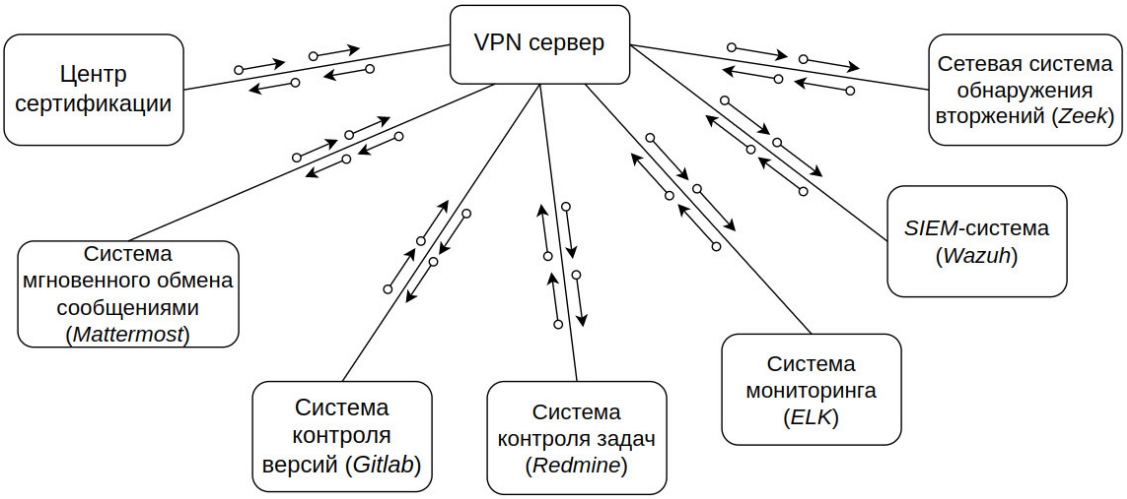

Рис. 2. Структурная диаграмма инфраструктуры технологического конвейера

Внедрение сетевой системы обнаружения вторжений (*англ. NIDS, Network Intrusion Detection System*) позволит повысить общий уровень защищенности предприятия и усложнит внедрение злоумышленника извне [9]. С этой целью предлагается использование *Zeek*, преимуществами которого являются возможность самостоятельной реализации модулей для покрытия большего числа вероятных сценариев поведения злоумышленника, а также функционал в части пассивного анализатора трафика стека протоколов *TCP/IP*, что в свою очередь значительно повышает уровень защищенности сети предприятия [10].

Своевременная реакция на возникающие инциденты важна для уменьшения издержек в случае проникновения злоумышленника в информационный контур предприятия. С этой целью предлагается внедрение системы сбора, анализа и идентификации корреляции событий (англ. *SIEM, Security information and event management)*, при помощи которой происходит управление событиями и информацией о безопасности вычислительной сети предприятия. Среди доступного на рынке программного обеспечения выбор был сделан в пользу *Wazuh*, ключевым отличием которого является проведение автоматизированного сканирования системы на предмет обнаружения вредоносного программного обеспечения или каких-либо других аномалий.

Нивелирование риска допуска ошибок по причине человеческого фактора обеспечивается использованием декларативной системы управления конфигурациями *Ansible*, гарантирующей консистентность, идемпотентность, а также воспроизводимость настройки инфраструктуры в соответствии с методологией *IaC*.

Обсуждение результатов

Многоэтапное тестирование каждого из компонентов разработанного программного комплекса по обеспечению информационной безопасности технологического конвейера разработки программных и аппаратно-программных реше-

ний было проведено с использованием средств автоматизации *GitlabCI*, интегрирующихся с системой версионирования *Gitlab*. Данный конвейер состоит из этапов проверки и анализа исходного кода, автоматического тестирования с использованием фреймворка *Molecule*, а также доставкой исправной версии программного обеспечения на производственный сервер (рис. 3).

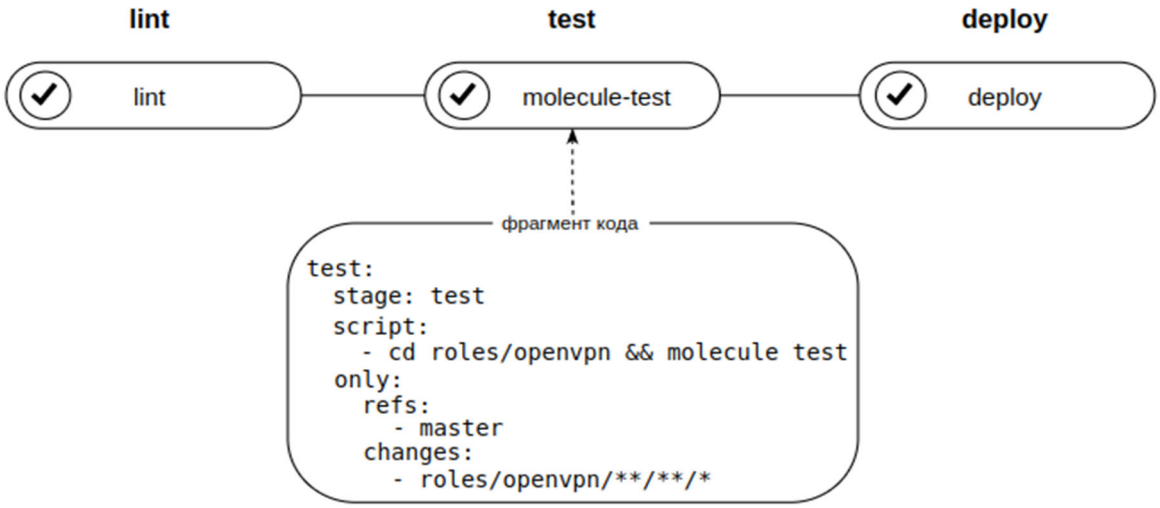

Рис. 3. Многоэтапный CI/CD конвейер фрагмента программного комплекса

Использование данных этапов тестирования позволило исключить риск возникновения ошибок по причине человеческого фактора при написании *Ansible*-ролей, что в свою очередь сказалось на уменьшении ошибок, возникающих на производственном сервере в среднем на 73% в ходе использования данного инструмента в ряде компаний. При этом было достигнуто сокращение сроков реализации проектов на 51%, что, в свою очередь, коррелирует с двукратным уменьшением издержек со стороны хозяйствующего субъекта.

Заключение

В рамках выполнения работы был спроектирован и программно реализован метод обеспечения информационной безопасности технологического конвейера разработки программных и аппаратно-программных решений, непрерывно поддерживающий в автоматическом режиме весь жизненный цикл проекта с обеспечением контроля качества, надежности, аутентичности и безопасности информационных ресурсов выпускаемой продукции. Предлагаемое решение включает комплексный подход к обеспечению локальной и сетевой безопасности на уровне приложений, хостов и сети (на всех уровнях стека протоколов *TCP/IP*). С этой целью интегрируются виртуальная частная сеть, системы обнаружения и предотвращения вторжений, сбора, анализа и корреляции событий, а также использование средств многослойной изоляции прикладного программного обеспечения.

Практическая значимость работы заключается в возможности уменьшения издержек со стороны предприятия, занимающегося разработкой программных и аппаратно-программных решений. Предлагаемый метод помогает повысить уровень надежности, отказоустойчивости и безопасности технических объектов и систем информационной инфраструктуры предприятия благодаря использованию комплексной автоматизации всех технологических процессов разработки с комбинированием существующих методик, инструментов и средств. При этом стоит отметить, что информационная безопасность инфраструктуры может быть обеспечена в пределах 98%, внедрение какого-либо количества средств защиты лишь усложняет процесс попадания злоумышленника в корпоративную инфраструктуру, но не исключает эту возможность.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Долинина О. Н. Управление процессом создания программного обеспечения систем принятия решений по критерию качества / О. Н. Долинина, А. Ф. Резчиков // Системы управления и информационные технологии. – 2017. – № 3(69). – С. 78-82. – EDN ZDGNBB.

2. F. M. A. Erich. A qualitative study of DevOps usage in practice / F. M. A. Erich, C. Amrit, M. Daneva // Journal of Software: Evolution and Process. 2017, Vol. 29, no.6. P.. 14-16.

3. Michael Hilton. Usage, costs, and benefits of continuous integration in open-source projects / Michael Hilton, Timothy Tunnell, Kai Huang, Darko Marinov, Danny Dig // ASE 2016: Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering. Singapore, 3-7 Sept. 2016. P. 426-435.

4. Долинина О. Н. Системный анализ, методы и модели построения интеллектуальных систем принятия решений при управлении сложными организационно-техническими комплексами: диссертация доктора техн. наук-Саратов, 2018.-247 с. – 2018.

5. Гаврилов А. Л. Способ защиты вычислительных сетей // Методическое пособие. – 2019.

6. Мерзликин А. Э. Анализ способов и средств защиты информации в локальных вычислительных сетях // Приоритеты и тенденции управления бизнес-процессами в структуре информационных систем. – 2019. – С. 267-272.

7. System of a self-organizing virtual secure communication channel based on stochastic multilayer encryption and overlay technologies / E. A. Basinya, Z. B. Akhayeva, D. H. Omarkhanova, G. B. Tolegenova [et al.]. – Text : direct // Journal of Theoretical and Applied Information Technology. - 2022. – Vol. 100, iss. 16. – P. 4918-4927.

8. Проектирование и реализация технологического конвейера разработки программного и аппаратно-программного обеспечения = Designing and implementation of the technological pipeline for the development of software and firmware / Е. А. Басыня, Е. А. Малышев. // Защита информации. Инсайд = Zasita informacii. Inside. – 2022. – № 5 (107). – С. 60–67.

9. Basinya E. A. Implementation of an intrusion detection and prevention system module for corporate network traffic management / E. A. Basinya, Y. K. Ravtovich // Актуальные проблемы электронного приборостроения (АПЭП–2018) = Actual problems of electronic instrument engineering (APEIE–2018) : тр. 14 междунар. науч.-техн. конф., Новосибирск, 2–6 окт. 2018 г. : в 8 т. – Новосибирск : Изд-во НГТУ, 2018. – Т. 1, ч. 6. – С. 178-183. - 45 экз. - ISBN (NSTU) 978-5-7782-3614-1.

10. Ажмухамедов И. М. Повышение безопасности компьютерных систем и сетей на основе анализа сетевого трафика / Ажмухамедов И. М., Марьенков А. Н. // Инфокоммуникационные технологии. – 2010. – Т. 8. – №. 3. – С. 106-108.