DOI 10.37882/2223-2966.2024.10.07

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ DEVSECOPS В УСЛОВИЯХ ПЕРЕХОДА НА ОТЕЧЕСТВЕННОЕ ПО: ПРОБЛЕМЫ И РЕШЕНИЯ

AUTOMATION OF DEVSECOPS PROCESSES IN THE CONTEXT OF THE TRANSITION TO DOMESTIC SOFTWARE: PROBLEMS AND SOLUTIONS

D. Bondar

Summary. One of the current urgent issues in the field of development and integration of innovative information technologies is ensuring data security and interaction with them. The presented article is devoted to the study of issues related to the integration of DevSecOps in modern conditions of transition to domestic software. The main purpose of the work is to form and highlight the most pressing problems of process automation through DevSecOps. Because of the work, the author systematized the key problems and presented the author's options for their solution. The materials of the article reveal several problems related to the threat of targeted attacks on the DevSecOps infrastructure in conditions of limited access to foreign security systems. Attention also focused on the problem of the lack of qualified information security specialists, especially in the context of domestic software and DevSecOps. The problem of the risk of data leakage and violation of confidentiality in the process of automation of DevSecOps also presented, and a practical implementation of the CI/CD pipeline configuration proposed, which contributes to monitoring and protection. The materials of the work can be useful for the modern field of information security, revealing key security issues in the automation of DevSecOps processes.

Keywords: information security, software, DevSecOps, threat, DDoS attack, monitoring, protection.

Бондарь Денис Евгеньевич
WB Bank Ops, DevOps-инженер,
ООО «ВБ ТЕХ», Россия, г. Москва
expacee@gmail.com

Аннотация. Одним из актуальных вопросов на текущий момент времени в области развития и интеграции инновационных информационных технологий является обеспечение безопасности данных и взаимодействия с ними. Представленная статья посвящена исследованию вопросов, связанных с интеграцией DevSecOps в современных условиях перехода на отечественное программное обеспечение. Основной целью работы является формирование и выделение наиболее актуальных проблем автоматизации процессов посредством DevSecOps. В результате работы автором систематизированы ключевые проблемы и представлены авторские варианты по их решению. Материалы статьи раскрывают целый ряд проблем, связанных с угрозой целенаправленных атак на инфраструктуру DevSecOps в условиях ограниченного доступа к зарубежным системам безопасности. Также внимание акцентировано на проблеме недостатка квалифицированных специалистов по информационной безопасности, особенно в контексте отечественного программного обеспечения и DevSecOps. Также представлена проблема риска утечки данных и нарушение конфиденциальности в процессе автоматизации DevSecOps, а также предложена практическая реализация конфигурации CI/CD pipeline, способствующая обеспечению мониторинга и защиты. Материалы работы могут быть полезны для современной сферы информационной безопасности, раскрывая ключевые вопросы безопасности при автоматизации процессов DevSecOps.

Ключевые слова: информационная безопасность, программное обеспечение, DevSecOps, угроза, DDoS-атака, мониторинг, защита.

Введение

Значимым результатом событий 2022 года стала необходимость импортозамещения программного обеспечения (далее — ПО). Данная тенденция не изменена в период 2024 года и является прямой необходимостью для российских компаний в современных условиях давления санкциями и политической нестабильности. Данные процессы включают не только разработку и интеграцию новых систем и инструментов обеспечения информационной безопасности (далее — ИБ), но и методологий, примером которой является DevSecOps [1]. Данным инструментом регулируются вопросы разработки, эксплуатации и защиты информации, при этом основное предназначение направлено на автоматизацию безопасности и интеграцию её на всех этапах жизненного цикла программного обеспечения, что становится критически важным для российских организаций, стремящихся поддерживать высокий уровень информационной безопасности.

Материалы представленной статьи посвящены ключевым проблемам, которые препятствуют российским компаниям повсеместно интегрировать DevSecOps в условиях перехода на отечественное ПО. Автором не только систематизируются ключевые проблемы, но также предлагаются решения для возможности их преодоления. Основное внимание уделено специфике информационной безопасности в России, а также возможностям использования open-source инструментов для достижения целей DevSecOps.

Материалы и методы

Для анализа проблем и решений, связанных с автоматизацией процессов DevSecOps в условиях перехода

на отечественное программное обеспечение, использованы результаты научных исследований отечественных авторов, а также обзоры и аналитические отчеты российских и международных экспертов в области информационной безопасности и разработки ПО. Особое внимание уделено публикациям, посвященным внедрению отечественного ПО в корпоративные и государственные структуры, а также специфическим проблемам, возникающим при интеграции DevSecOps-подходов в условиях ограничений на использование зарубежных технологий. Использована динамика развития технологий и трендов в IT-сфере на протяжении последних лет, с акцентом на период до 2024 года, что позволило учесть, как текущие тенденции, так и будущие вызовы в данной области.

Методологическая основа исследования включает сравнительный анализ проблем и решений автоматизации DevSecOps в контексте импортозамещения ПО. Использованы методы системного анализа для определения ключевых факторов, влияющих на эффективность автоматизации, а также методы экспертного опроса и интервью с представителями отечественных компаний, внедряющих DevSecOps в условиях перехода на отечественные решения. Помимо этого, проведен анализ существующих инструментов и практик автоматизации, адаптированных под отечественные реалии, с целью выявления их преимуществ и недостатков в сравнении с зарубежными аналогами.

Обзор литературы

Методология DevSecOps основывается на идее включения процессов безопасности в непрерывную интеграцию и доставку программного обеспечения (CI/CD) [2]. Традиционно DevOps фокусируется на ускорении разработки и выпуска программного обеспечения, но с увеличением числа кибератак на этапе разработки и эксплуатации стало очевидно, что вопросы безопасности должны быть интегрированы на каждом этапе жизненного цикла ПО.

Международные исследования показывают, что автоматизация процессов безопасности на ранних этапах разработки позволяет значительно снизить количество уязвимостей и повысить безопасность конечных решений [3]. Однако в российском контексте переход на отечественные решения создает дополнительные проблемы, так как многие инструменты, доступные на западном рынке, недоступны или ограничены в России.

Отечественные разработки в области DevSecOps, такие как платформы управления Kubernetes-кластерами (например, Deckhouse) и системы CI/CD (например, GitLab CE), являются перспективными, но требуют значительных усилий по их адаптации и интеграции в существующие процессы [4]. Сочетание этих факторов требует поиска новых решений для обеспечения безопасности и автоматизации в условиях российских реалий.

Результаты

Далее представлены результаты анализа наиболее значимых проблем и вызовов внедрения DevSecOps в России на момент 2024 года:

Проблема 1: Угроза целенаправленных атак на инфраструктуру DevSecOps в условиях ограниченного доступа к зарубежным системам безопасности — одной из ключевых проблем в условиях санкций является ограничение доступа российских компаний к зарубежным инструментам безопасности. Например, платформы Azure Security Center, AWS Shield и многие другие, ранее предоставляли мощные средства защиты от DDoS-атак, обнаружения угроз и управления инцидентами [5]. Однако из-за санкций использование этих инструментов стало невозможным для российских компаний, что создает значительные риски, особенно для критической инфраструктуры и государственных организаций. Переход на отечественное ПО требует создания новых механизмов защиты, которые смогут заменить западные решения. Отечественные облачные платформы и решения в сфере безопасности еще недостаточно зрелы, что увеличивает вероятность целенаправленных атак и усложняет защиту инфраструктуры.

Решение: Zero Trust и разработка собственных систем IDS/IPS — одним из решений является внедрение подхода Zero Trust, который предполагает недоверие ко всем элементам системы, как внутри, так и за её пределами. Этот подход позволяет минимизировать риск компрометации даже в случае взлома одного из элементов инфраструктуры [6]. Дополнительно рекомендуется интеграция собственных систем обнаружения и предотвращения атак (IDS/IPS) на базе open-source решений. Например, Suricata и Zeek — это мощные инструменты для мониторинга сетевого трафика и обнаружения аномалий, которые можно адаптировать для использования в отечественной инфраструктуре. Эти системы могут быть интегрированы с отечественными облачными платформами и обеспечивать многоуровневую защиту от атак.

Проблема 2: Недостаток квалифицированных специалистов по информационной безопасности, особенно в контексте отечественного ПО и DevSecOps — дефицит специалистов по информационной безопасности становится всё более острой проблемой в России, особенно в контексте перехода на отечественное ПО и новые инструменты DevSecOps. Множество экспертов были обучены работе с западными решениями, и их адаптация к новым отечественным инструментам требует времени и ресурсов. Это увеличивает риск ошибок и нарушений безопасности из-за человеческого фактора.

Решение: Программы обучения и сертификации, ориентированные на российские решения — для решения этой проблемы необходима разработка специализированных программ обучения и сертификации, направленных на освоение отечественных технологий и инструментов [7]. Компании могут создавать внутренние программы повышения квалификации и организовывать регулярные тренинги для своих специалистов. Также следует развивать сотрудничество между образовательными учреждениями и бизнесом для подготовки молодых специалистов, которые будут готовы работать с отечественными решениями и интегрировать DevSecOps в российских условиях [8]. Например, создание учебных лабораторий по DevSecOps на базе российских вузов позволит готовить кадры, которые смогут эффективно работать в условиях перехода на отечественное ПО.

Проблема 3: Риск утечки данных и нарушение конфиденциальности в процессе автоматизации DevSecOps — одной из наиболее серьезных угроз в условиях автоматизации DevSecOps является риск утечки данных и нарушение конфиденциальности. Данный риск увеличивается при использовании новых отечественных инструментов, которые могут быть недостаточно зрелыми или не обеспечивать необходимые уровни защиты [9]. Особенно актуальна данная проблема для компаний, работающих в секторах с высокими требованиями к безопасности, таких как финансы, здравоохранение и государственные структуры. Утечки данных или компрометация критически важных систем могут привести к серьезным последствиям, включая финансовые потери и ущерб репутации.

Решение: Внедрение отечественных криптографических решений и улучшение политик конфиденциальности — для защиты данных необходимо использовать отечественные криптографические решения, которые сертифицированы Федеральной службой безопасности (ФСБ) и Федеральной службой по техническому и экспертному контролю (ФСТК) России. Эти решения могут обеспечить достаточно высокий уровень защиты данных на всех подуровнях инфраструктуры, включая данные при хранении и в процессе передачи [10]. Также следует разработать и внедрить строгие политики конфиденциальности данных, включая контроль доступа, аудит использования данных и автоматическое удаление по истечении срока хранения. Интеграция механизмов шифрования на уровне контейнеров и виртуальных машин позволит снизить риск утечек данных и повысить общую безопасность системы.

Для возможности обеспечения безопасности данных автором предлагается техническая реализация DevSecOps с использованием отечественного программного обеспечения. Так, в условиях перехода на отечественное ПО автоматизация DevSecOps требует использования комбинации отечественных и open-source решений. Далее автором представлен пример архитектуры DevSecOps, которая сочетает использование платформы Deckhouse для управления Kubernetes-кластерами и бесплатной версии GitLab CE для CI/CD процессов. Основными элементами архитектуры являются Deckhouse, GitLab CE, Trivy, Suricata и Zeek. На рис. 1 представлен подробный состав архитектуры.

Данная архитектура позволит обеспечить полный цикл автоматизации DevSecOps, включая сборку, тестирование, анализ безопасности и развертывание приложений в контейнерах. Интеграция процессов безопасности в CI/CD pipeline позволяет снизить количество

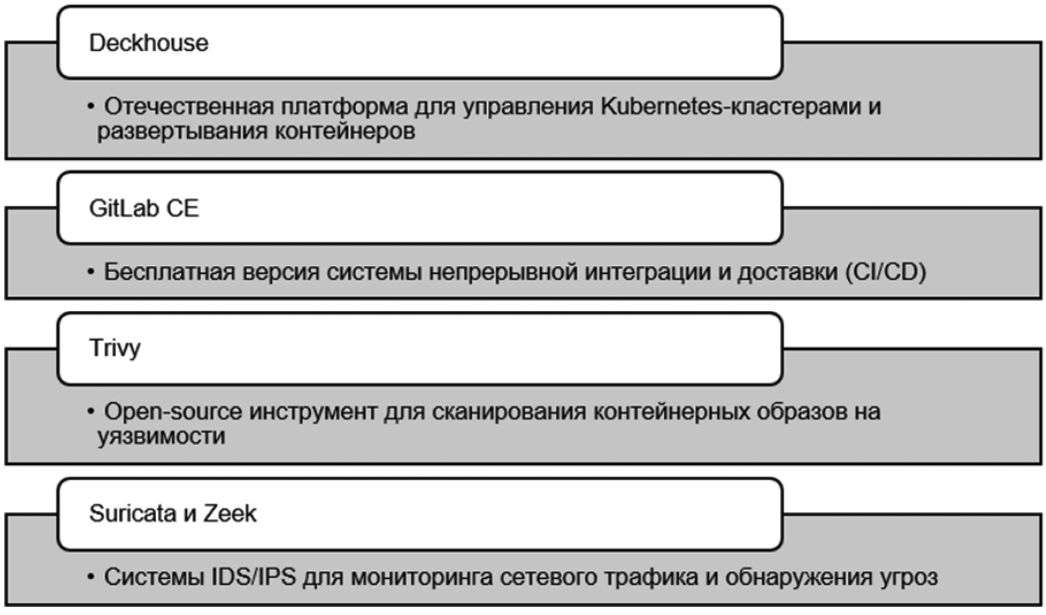

Рис. 1. Основные элементы архитектуры

уязвимостей и оперативно реагировать на инциденты безопасности. Далее представлен пример конфигурации CI/CD pipeline, включающий этапы безопасности:

```yaml
stages:
  — build
  — test
  — security
  — deploy

build_job:
  stage: build
  script:
    — docker build -t $CI_REGISTRY_IMAGE: $CI_
COMMIT_REF_NAME .

test_job:
  stage: test
  script:
    — pytest tests/

sast_job:
  stage: security
  image: sonarsource/sonar-scanner-cli
  script:
    — sonar-scanner

image_scan:
  stage: security
  image: aquasec/trivy:latest
  script:
    — trivy image --severity HIGH, CRITICAL $CI_
REGISTRY_IMAGE: $CI_COMMIT_REF_NAME

deploy_job:
  stage: deploy
  script:
    — kubectl apply -f deployment.yaml
```

Этот pipeline включает автоматическую сборку Docker-образов, запуск тестов, статический анализ кода (SAST) с использованием SonarQube, сканирование контейнерных образов на уязвимости с помощью Trivy и развертывание приложения в Kubernetes-кластере через Deckhouse.

В дополнение к автоматизации процессов разработки и развертывания необходимо интегрировать системы мониторинга и обнаружения угроз. Например, Suricata может использоваться для мониторинга сетевого трафика и обнаружения подозрительной активности, а Zeek — для детального анализа событий и их корреляции с другими данными. Эти инструменты могут быть настроены для интеграции с системами оповещения и автоматической реакции на инциденты безопасности, что позволит оперативно реагировать на угрозы и минимизировать возможные последствия атак.

Авторский вариант интеграции Suricata и Zeek с инфраструктурой DevSecOps выглядит следующим образом:

1. Установка и настройка Suricata на уровне сети для мониторинга всех входящих и исходящих соединений. Suricata может быть настроена на обнаружение аномалий и фильтрацию подозрительного трафика. Например, если будет обнаружен подозрительный IP-адрес или определенный вид атаки (например, попытки SQL-инъекций), система автоматически оповестит администратора или заблокирует трафик.
2. Использование Zeek для анализа логов событий, таких как попытки авторизации, загрузка подозрительных файлов или необычное поведение пользователей. Zeek может собирать метаданные сетевого трафика и помогать в анализе сложных инцидентов безопасности, таких как многоэтапные атаки.
3. Интеграция с системами оповещения (например, Prometheus, Grafana или ELK) для визуализации событий и получения уведомлений в реальном времени. Это позволяет безопасникам и DevOps-командам оперативно отслеживать состояние системы и принимать необходимые меры.

При этом важно обеспечить дополнительные аспекты безопасности, включающие шифрование данных. Все данные должны быть зашифрованы как при хранении, так и при передаче. Это включает использование сертифицированных криптографических алгоритмов и управление ключами через отечественные или open-source решения (например, HashiCorp Vault). Также следует учесть возможность аутентификации и управления доступом. Настройка строгих политик доступа, включая многофакторную аутентификацию (MFA), является ключевой составляющей при доступе к критическим системам. Для управления доступом возможно использование таких решений, как Keycloak или иных отечественных аналогов.

Заключение

Автоматизация DevSecOps при переходе на отечественное программное обеспечение — ключевая задача для российских организаций, стремящихся сохранить высокий уровень кибербезопасности. В материалах работы рассмотрены ключевые проблемы интеграции DevSecOps на момент 2024 года, которыми стали: ограниченный доступ к зарубежным инструментам; нехватка квалифицированных кадров; риски утечек данных. В ре-

зультате автором предложены практические решения для их преодоления.

Ключевым выводом работы стало то, что использование отечественного и open-source ПО (Deckhouse, GitLab CE, Trivy, Suricata, Zeek) позволит создать безопасную инфраструктуру, соответствующую современным требованиям. Интеграция безопасности на всех этапах жизненного цикла разработки минимизирует уязвимости и ускоряет реакцию на угрозы. При этом успешная реализация DevSecOps требует внедрения таких подходов, как Zero Trust, и автоматизации на основе мониторинга и анализа данных. Необходимо также развитие образовательных программ для подготовки специалистов, способных работать с отечественными решениями. В заключение необходимо отметить, что будущее DevSecOps в России зависит от способности компаний эффективно адаптироваться к новым условиям, обеспечивая защиту своих информационных систем и данных в рамках перехода на отечественное ПО.

ЛИТЕРАТУРА

1. Ковальчук О.Н., Романова Т.В. DevSecOps: Современные методы интеграции безопасности в процессы DevOps. Информационная безопасность. 2021. №5(2). С. 12–18.
2. Петров А.В., Смирнов В.А. Внедрение Zero Trust архитектуры в российских компаниях. Информационные технологии и безопасность. 2020. № 7(3). С. 45–52.
3. Федоров М.С. Актуальные вопросы автоматизации безопасности на этапах разработки ПО. Программирование и защита данных. 2019. № 8(1). С. 34–40.
4. Иванова Е.П., Сидоров Д.В. Кибербезопасность в условиях санкционного давления: Влияние на российские компании. Журнал информационной безопасности. 2022. № 6(4). С. 25–30.
5. Смирнова И.А., Михайлов П.К. Адаптация open-source решений для обеспечения безопасности в российских условиях. Информационные технологии и управление. 2023. № 9(2). 61–67.
6. Безпятый М.В. Автоматизация и оптимизация процессов разработки и развертывания в DevOps: применение современных методов и инструментов // Инновации и инвестиции. 2023. №7. С. 458–464.
7. Сухомлин В.А. Система международной стандартизации в области ит, ее роль в развитии информационной индустрии и принципы функционирования // Современные информационные технологии и ИТ-образование. 2022. №2. С. 412–440.
8. Заяц Е.А. Автоматизация и оптимизация процессов разработки по для вычислительной техники // Инновации и инвестиции. 2023. №6. С. 152–155.
9. Никифоров А.В. Как внедрение непрерывной интеграции и тестирование помогает обеспечить соответствие требованиям при разработке программного продукта // International journal of professional science. 2023. №4. С. 88–96.
10. Тюменцев Д.В. Автоматизация тестирования в DevOps: подходы и лучшие практики // Международный журнал гуманитарных и естественных наук. 2024. №2–2. С. 156–159.

Журнал «Современная наука: актуальные проблемы теории и практики»