ЗАВИСИТ ОТ ЦЕЛИ

ОЦЕНКА ПРОЦЕССОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

Сергей КАНИВЕЦ
ведущий консультант отдела
консалтинга АО «ДиалогНаука»

Безопасность программного обеспечения (ПО) играет критически важную роль в условиях современной цифровой экономики. Регулярные кибератаки, утечки данных и нарушения конфиденциальности негативно влияют как на коммерческие организации, так и на государственные структуры. Одним из ключевых факторов повышения уровня защиты является корректная организация процессов разработки безопасного ПО. Однако разработка безопасного ПО — это не только внедрение технических мер защиты, но и организация процесса с акцентом на управление рисками, соответствие требованиям регуляторов и обучение специалистов. В данной статье рассмотрены основные методики и подходы к оценке процессов безопасной разработки.

МЕТОДИКИ ОЦЕНКИ ПРОЦЕССОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Оценка процессов разработки безопасного ПО является важным этапом для создания защищённых программных продуктов, направленным на проверку соответствия процессов современным стандартам, выявление слабых мест и разработку корректирующих мер. Сейчас уже существует множество подходов и инструментов для оценки зрелости процессов разработки, например OWASP SAMM, DevSecOps Maturity Model и Synopsys BSIMM, позволяющие не только оценить текущее состояние, но и наметить пути его улучшения. Рассмотрим особенности каждой из этих моделей.

OWASP Software Assurance Maturity Model (SAMM) — это нормативная или предписывающая модель, которая структурирует процессы разработки безопасного ПО. Она включает 15 практик, разделённых на пять бизнес-функций: Governance, Design, Implementation, Verification и Operation. Каждая практика состоит из двух потоков: A — «поверхностный» и B — «углублённый», что позволяет выбирать степень детализации. SAMM обеспечивает формализацию и измерение результатов, минимизируя затраты на оценку. Компания самостоятельно определяет целевой уровень зрелости в удобном для неё горизонте планирования: от одного до пяти лет. Для автоматизации оценки компания может использовать доступные инструменты, такие как SAMMwise или SAMMY.

OWASP DevSecOps Maturity Model (DSOMM) описывает практики, направленные на интеграцию безопасности в процессы разработки и CI/CD. Модель выделяет пять инструментов: Build and Deployment, Culture and Organization, Implementation, Information Gathering, Test and Verification, каждый из которых включает меры защиты, распределённые по пяти уровням зрелости.

Synopsys BSIMM — это описательная модель, базирующаяся на практике 130 организаций. Она состоит из четырёх доменов, каждый из которых включает три практики, разделённые на три уровня покрытия. BSIMM позволяет компаниям сравнивать свои достижения с общепринятыми в индустрии практиками, реализованными у лидеров рынка, а доступные инструменты облегчают процесс оценки.

КОНЦЕПЦИЯ ОЦЕНКИ ПРОЦЕССА РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Центральное место в этой концепции занимает системный подход, который позволяет структурировать и интегрировать меры безопасности на всех уровнях. В основе такого подхода лежит идея цикличности и непрерывного совершенствования, что обеспечивает устойчивость к новым угрозам и адаптацию к меняющимся условиям.

Управление процессом безопасной разработки является основой для обеспечения системного подхода к защите программного обеспечения. Оно охватывает ключевые аспекты управления — от стратегического планирования до контроля и оценки соответствия, что обеспечивает комплексное внедрение мер безопасности на всех этапах разработки, в том числе позволяет оценить текущее состояние процессов по следующим направлениям:

- описание стратегии и планирование процесса разработки (так как эффективное управление начинается с формулирования стратегии, которая определяет долгосрочные цели

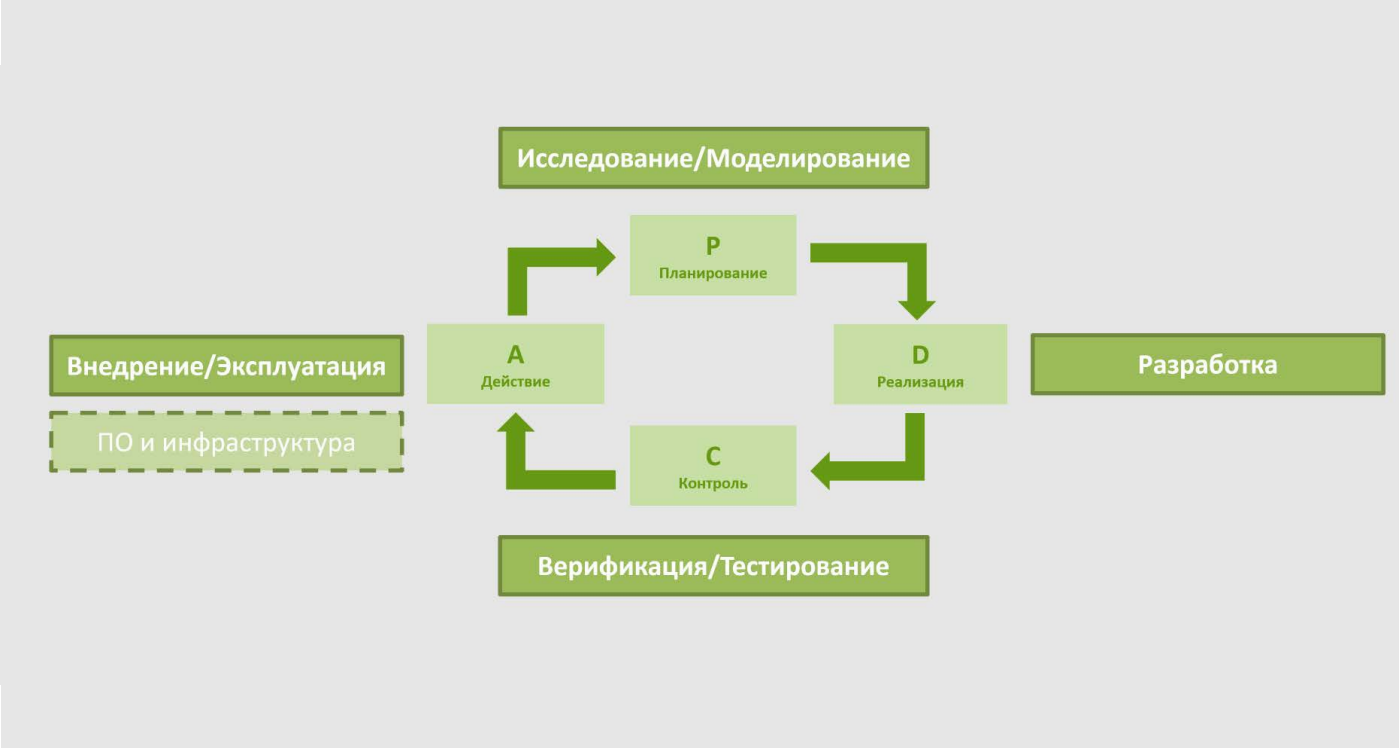

Рисунок 1. Соответствие элементов цикла PDCA мерам, относящимся к процессам безопасной разработки ПО

и задачи, в том числе в области разработки безопасного ПО);

- метрики эффективности (позволяют измерить и оценить текущий уровень безопасности разработки, а также отслеживать прогресс);
- повышение осведомлённости и квалификации (обучение персонала играет ключевую роль в предотвращении ошибок, связанных с безопасностью);
- контроль (контроль должен охватывать все аспекты процессов разработки и помогает обеспечить соблюдение установленных стандартов);
- оценка соответствия (эта часть включает проверку соответствия процессов безопасной разработки установленным стандартам и законодательным требованиям).

Цикл PDCA (планирование — реализация — контроль — действие) является универсальной моделью управления процессами, которая может быть применима и к процессам разработки безопасного ПО. В контексте обеспечения безопасности PDCA помогает систематизировать и интегрировать защитные меры на всех этапах жизненного цикла продукта (рис. 1).

Каждый элемент цикла включает набор ключевых мер и действий, по которым оцениваются процессы:

1. Планирование (PLAN) — этап исследования и моделирования:

- подготовка требований;
- моделирование угроз / оценка рисков;
- требования безопасности при использовании зависимостей;
- проектирование архитектуры.

2. Реализация (DO) — этап разработки ПО:

- управление конфигурацией ПО;
- требования к безопасности системы сборки и раскатки ПО;
- безопасность инфраструктуры разработки и тестирования;
- обеспечение целостности кода.

3. Контроль (CHECK) — этап верификации и тестирования:

- оценка архитектуры;
- анализ кода;
- тестирование защищённости.

4. Действие (ACT) — этап внедрения и эксплуатации:

- внедрение и эксплуатация (подготовка, доставка, вывод из эксплуатации);
- безопасность инфраструктуры (эксплуатация инфраструктуры ПО, тестирование на проникновение, управление уязвимостями, управление инцидентами).

ВЫВОДЫ

Выбор методики оценки зависит от целей организации: стремление достичь определённого уровня зрелости или соответствие международным стандартам. Использование моделей OWASP SAMM, DSOMM или BSIMM позволяет выявить слабые места в процессах и разработать долгосрочные стратегии совершенствования. Это обеспечивает соответствие требованиям безопасности, сокращает риски и укрепляет доверие пользователей. Представленная концепция возможна к применению и для новой редакции национального стандарта ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Применение таких подходов делает процессы разработки ПО более надёжными и способствует достижению высокого уровня защищённости, соответствующего мировым стандартам.