

Secure Development Principles

Публичные принципы безопасной разработки и контролируемого выпуска программных изменений.

Код документа	VIR-PUB-SDLC-001
Категория	Информационная безопасность и разработка
Публикация	27.09.2026 • версия 1.0 • действует до замены новой редакцией

Публичная версия. Предназначена для размещения на сайте и предоставления заказчикам и партнёрам. Не содержит конфиденциальных технических деталей и не заменяет договорные условия или внутренние регламенты.

Связанные материалы: virtek.pro/trust-center • virtek.pro/services/custom-software • virtek.pro/documents

1. Подход

ВирТЭК рассматривает безопасность как свойство всего жизненного цикла программного решения. Набор конкретных мер определяется архитектурой, данными, критичностью, моделью размещения и требованиями проекта.

2. Базовые практики

- разделение сред разработки, тестирования и промышленной эксплуатации там, где это требуется архитектурой и риском;
- управление секретами без размещения паролей, ключей и токенов в исходном коде или общедоступных конфигурациях;
- контроль зависимостей и происхождения используемых компонентов;
- проверка значимых изменений до выпуска и контролируемое продвижение версии в промышленную среду;
- журналирование релевантных событий и действий для диагностики и расследования;
- управление доступом к репозиториям, средам сборки и выпуску по принципу минимальной необходимости.

3. Изменения и выпуск

1. Изменение получает понятную цель и область влияния.
2. Оцениваются зависимости, влияние на данные, доступы, интеграции и безопасность.
3. Изменение проходит предусмотренную проектом проверку и тестирование.
4. Для значимого выпуска определяется способ отката или восстановления.
5. Выпуск выполняется контролируемо; результат проверяется после внедрения.
6. Документация, конфигурация и эксплуатационные сведения актуализируются при необходимости.

4. Уязвимости и зависимости

Уязвимости и значимые обновления рассматриваются с учётом критичности, применимости, влияния на совместимость и риска простоя. Исправление должно сопровождаться проверкой результата; исключения фиксируются и пересматриваются.

5. Данные и секреты

Исходный код, архитектура, конфигурации, ключи доступа, отчёты об уязвимостях и иные чувствительные материалы рассматриваются как информация ограниченного доступа в соответствии с их категорией. Секреты не должны становиться частью обычного исходного кода или публичных артефактов сборки.

6. Производственный доступ

Разработка сама по себе не даёт автоматического права на административный доступ к промышленной среде. Доступ, изменение конфигурации и аварийные действия регулируются отдельными ролями и процессами эксплуатации/изменений.

7. Границы документа

Публичный уровень

Документ описывает инженерные принципы и не утверждает универсальный набор инструментов или одинаковый процесс для всех проектов. Конкретные SDLC-контроли, тесты, CI/CD и критерии приёмки фиксируются для соответствующей системы.

Публикация и актуализация

Актуальная редакция документа публикуется на сайте ВирТЭК. Документ пересматривается при существенном изменении процессов, архитектуры, законодательства, договорной модели или требований заказчиков.

Актуальная версия: virtek.pro/documents