Регламент по безопасной разработке программного обеспечения

Версия	1.0
Дата вступления в силу	18 декабря 2025 г.
Срок действия	Бессрочно с обязательным пересмотром не реже 1 раза в год
Ответственный за соблюдение	Руководитель отдела разработки

1. Общие положения

1.1. Настоящий регламент устанавливает обязательные требования и процедуры на всех этапах жизненного цикла программного обеспечения от проектирования до сопровождения — с целью обеспечения безопасности, целостности, конфиденциальности и соответствия нормативным актам.

1.2. Регламент распространяется на всех участников процесса разработки: разработчиков, архитекторов, DevOps-инженеров, тестировщиков, аналитиков и менеджеров проектов.

1.3. Невыполнение требований настоящего документа влечет за собой дисциплинарную ответственность и может повлечь ограничение доступа к инфраструктуре организации.

2. Инфраструктура разработки

2.1. CI/CD-конвейер

2.1.1. Все изменения проходят через автоматизированный CI/CD.

2.1.2. Запрещено ручное развертывание в production без прохождения всех этапов пайплайна.

2.1.3. Конфигурации CI/CD хранятся в системе контроля версий.

2.2. Логирование и мониторинг

2.2.1. Все компоненты генерируют структурированные логи в формате JSON.

2.2.2. Обязательно сквозное логирование с уникальным идентификатором запроса.

2.2.3. Production-логи имеют уровень не ниже INFO и (или) DEBUG — только временно и по согласованию.

2.2.4. Системы мониторинга (например, Prometheus, Grafana, ELK и др.) обязательны на всех средах по усмотрению заказчика.

2.3. Управление секретами

2.3.1. Секреты хранятся исключительно в специализированных хранилищах (например, HashiCorp Vault, AWS Secrets Manager и др.) по усмотрению заказчика.

2.3.2. Запрещено размещение секретов в коде, конфигурационных файлах, .env, .gitignore или переменных CI/CD без шифрования.

2.4. Контроль доступа (RBAC)

2.4.1. Все сервисы реализуют авторизацию на основе ролей.

2.4.2. Применяется принцип минимальных привилегий.

2.4.3. Все действия пользователей и систем сохраняются в журнале событий.

3. Работа с данными

3.1. Валидация и санитизация

3.1.1. Все внешние данные проходят строгую валидацию, нормализацию и очистку.

3.1.2. Запрещено прямое использование пользовательского ввода в SQL, шаблонах, командах ОС.

3.2. Обработка чувствительных данных

3.2.1. Персональные данные и иные чувствительные данные подлежат шифрованию и / или маскированию.

3.2.2. Передача персональных данных за пределы РФ допускается только при соблюдении требований ФЗ-152 и согласия субъекта.

3.3. Целостность и аудит

3.3.1. Изменения данных — только транзакционные и идемпотентные.

3.3.2. Все операции фиксируются в аудит-логах с указанием субъекта, времени, типа и результата действия.

4. Безопасность кода

4.1. Статический анализ (далее - SAST)

4.1.1. Все merge/pull request проходят SAST.

4.1.2. Уязвимости уровня Критическое / Высокое, Critical / High блокируют слияние.

4.2. Управление зависимостями (далее - SCA)

4.2.1. Все сторонние библиотеки сканируются на уязвимости.

4.2.2. Патчи по критическим уязвимостям применяются в течение 7 календарных дней.

4.3. Тестирование

4.3.1. Покрытие unit-тестами — не менее 80% бизнес-логики.

4.3.2. Интеграционные тесты включают сценарии безопасности (например, аутентификация, авторизация, обработка ошибок).

4.3.3. DAST-сканирование (например, OWASP ZAP, Burp Suite) и пентесты — не реже 1 раза в квартал по усмотрению заказчика.

5. Продуктовая аналитика и метрики

5.1. Сбор поведенческих метрик обязателен для всех новых функций.
5.2. Персональные данные в аналитике подлежит анонимизации или агрегированию до не идентифицируемого уровня.
5.3. Все отчеты должны содержать описание источника данных, методики расчета и частоту обновления.

6. Управление инцидентами и соответствие

6.1. Реагирование на инциденты

6.1.1. Время обнаружения и классификации критического инцидента — не более 15 минут.

6.1.2. Время начала сдерживания — не более 1 час.

6.1.3. Проводится анализ с фиксацией корневых причин и мер предотвращения.

6.2. Соответствие нормативным требованиям РФ

6.2.1. Все процессы должны соответствовать ФЗ РФ, а также установленным стандартам ГОСТ РФ.

6.2.2. При работе с финансовыми организациями реализуется дополнительный уровень защиты в соответствии с требованиями ЦБ РФ к критической ИТ-инфраструктуре.

6.3. Моделирование угроз

6.3.1. Для каждого нового модуля или микросервиса до начала разработки проводится threat modeling.

6.3.2. Формируется Data Flow Diagram и матрица рисков с мерами снижения.

7. Сокращения и терминология

Сокращение	Расшифровка	Определение
ПО	Программное обеспечение	Совокупность программ, данных и документации для выполнения задач на вычислительных системах.
CI/CD	Continuous Integration / Continuous Delivery	Автоматизированный процесс сборки, тестирования и доставки ПО.

Сокращение	Расшифровка	Определение
SAST	Static Application Security Testing	Анализ исходного кода на уязвимости без выполнения.
DAST	Dynamic Application Security Testing	Тестирование работающего приложения на уязвимости.
SCA	Software Composition Analysis	Анализ сторонних зависимостей на уязвимости и лицензионные риски.
RBAC	Role-Based Access Control	Модель управления доступом на основе ролей.
PII	Personally Identifiable Information	Персональные данные, позволяющие идентифицировать субъекта.
PCI	Payment Card Industry Data	Данные платежных карт, регулируемые PCI DSS.
Prod	Production	Боевая среда, доступная пользователям.
Staging	—	Предпродакшн-среда, копия production.

Сокращение	Расшифровка	Определение
Dev	Development	Среда локальной разработки.
KPI	Key Performance Indicator	Ключевой показатель эффективности.

7.1. Все аббревиатуры при первом упоминании в тексте (кроме таблиц и заголовков) расшифровываются.

7.2. Введение новых терминов требует согласования с СТО и внесения в глоссарий.

8. Ответственность, обучение и контроль

8.1. Руководитель разработки несет ответственность за соблюдение регламента.

8.2. Отдел информационной безопасности проводит аудиты каждые 6 месяцев.

8.3. Все сотрудники проходят:

8.3.1. первоначальное обучение при трудоустройстве;

8.3.2. ежегодное обучение и тестирование по актуальным угрозам и безопасному программированию.

8.4. Нарушения фиксируются, расследуются и влекут дисциплинарные меры вплоть до прекращения доступа.

Подпись ответственного лица:

_____ _____ _____

[дата] [подпись] [ФИО, должность]