Этап	I. Собственная разработка	II. Заказная разработка	III. Вендорская разработка
1. Анализ, планирование	I.1.1 Моделирование угроз I.1.2 Ревью безопасности архитектуры ПО I.1.3 Формирование требований безопасности	II.1.1 Формирование раздела по безопасности в ТЗ	III.1.1 Анализ имеющихся функций безопасности ПО III.1.2 Доработка ПО вендором по требованиям безопасности* * - при наличии соответствующей возможности
2. Написание кода	I.2.1 Защита исходного кода I.2.1.1 Доступы к исходному коду I.2.1.2 Обеспечение целостности исходного кода I.2.1.3 Поиск секретов I.2.2 SCA I.2.2.1 Проверка достоверности источника получения I.2.2.2 Проверка репутации разработчика заимствованного компонента I.2.2.3 Формирование SBOM I.2.2.4 Проверка политики лицензирования I.2.3 SAST I.2.4 Обеспечение ИБ среды разработки (базовая защита)	II.2.1 Получение выписок из отчетов SAST II.2.2 Получение выписок из отчетов SCA	III.2.1 Запрос у вендора выписок из отчетов о SAST* III.2.2 Запрос у вендора выписок из отчетов о SCA* * - при наличии соответствующей возможности
3. Сборка	I.3.1 Защита пайплайна CI/CD I.3.2 Защита артефактов I.3.2.1 Использование КС и ЭП I.3.2.2 Управление секретами (ключевой информацией и сертификатами) I.3.2.3 Шифрование критически важных артефактов I.3.3 Безопасное развертывание	II.3.1 Получение лога сборки	–
4. Тестирование	I.4.1 Настройка базовых автотестов I.4.2 Функциональное тестирование I.4.3 DAST I.4.4 Пентест (в том числе применение intercepting proxy) I.4.5 Обеспечение ИБ тестовой среды (базовая защита)	II.4.1 Получение выписок из отчетов о тестировании (покрытие кода и т.д.) II.4.2 Получение выписок из отчетов DAST II.4.3 Получение выписок из отчетов о пентесте	III.4.1 Запрос у вендора отчетов о тестировании
5. Развертывание	5.1 Обеспечение ИБ продовой среды (расширенная защита)		
	I.5.2 Безопасность контейнеров и оркестраторов	II.5.2 Входной контроль ПО («белый ящик», «серый ящик»**) II.5.3 Проверка всех КС и ЭП ** - при отсутствии лицензионных ограничений со стороны вендора	III.5.2 Входной контроль ПО («серый ящик», «черный ящик») III.5.3 Проверка всех КС и сертификатов
6. Эксплуатация	6.1 WAF		
	6.2 RASP		–
7. Мониторинг	7.1 SIEM		

AKTIV. CONSULTING