Чек-лист ИБ-требований к подрядчику для ГИС
Приказ ФСТЭК России № 117

Чек-лист предназначен для проверки полноты требований к подрядчику, выполняющему разработку или модернизацию ПО для государственных информационных систем.
Составлен на основе Приказа ФСТЭК России № 117 и ГОСТ Р 56939-2024.
Чек-лист содержит требования к процессам безопасной разработки, необходимый объем документирования и варианты реализации.
С его помощью можно проверить, какие требования уже закрыты, а какие требуют доработки в ТЗ и контракте.

Раздел	Пункт из 117 приказа	Требование из ГОСТ-56939	Что защищаем (объект защиты)	Требование	Требование к документированию	Требование к усилению	Реализация on-prem	Выполнение с помощью Apsafe
1. Нормативное соответствие процессов (ГОСТ)								
Процесс разработки	3.12.1	5.1	Процесс разработки ПО	Разработать и утвердить регламент безопасной разработки: роли, процессы, артефакты	Внутренний регламент по разработке безопасного программного обеспечения. Состав ПО. Перечень подразделений (работников), на которых возложены функции по организации и внедрению процессов разработки безопасного программного обеспечения, их функции и полномочия	-	Внедрение необходимых инструментов и процессов РБПО силами УЦСБ, обучение сотрудников Заказчика (если требуется), разработка регламента	Все необходимые практики реализуются с помощью сервиса Apsafe, УЦСБ разрабатывает регламент РБПО с указанием Apsafe
Процесс разработки	3.12.2	5.1	Процесс разработки ПО	Планирование мероприятий по разработке безопасного программного обеспечения	В регламенте должны быть описаны планируемые мероприятия и их периодичность	-	Разрабатывается дорожная карта	Разрабатывается дорожная карта с учетом подключения к Apsafe
Процесс разработки	3.12.3	5.2	Процесс разработки ПО	Обучение работников, осуществляющих разработку, поддержку безопасного программного обеспечения	В регламенте должны быть описаны: перечень подразделений и порядок обучения (периодичность, формы)	-	Проводится обучение разработчиков правилам безопасного кодирования	
Архитек-тура	3.12.4	5.3	Архитектура и компоненты системы	Формирование и предъявление требований по безопасности к программному обеспечению, включая требования к его архитектуре	Требования к безопасности должны быть зафиксированы в регламенте или отдельном документе (техническом задании)	-	УЦСБ разрабатывает модель угроз и на ее основе рекомендации к архитектуре ПО с учетом требований ИБ	
Архитек-тура	3.12.5	5.4	Архитектура и компоненты системы	Управление конфигурацией программного обеспечения	В регламенте должен быть описан порядок управления конфигурацией и перечень используемых инструментов	-	Разрабатывается регламент Управления конфигурацией	
Безопас-ное коди-рование	3.12.6	5.5	Исходный код	Управление недостатками и запросами на изменение безопасного программного обеспечения	Процедура управления недостатками должна быть описана в регламенте	-	Разрабатывается регламент Управления изменениями	
2. Инструментальный анализ кода								
Безопас-ное коди-рование	3.12.7	5.9	Исходный код	Обязательное security code review для всех изменений	В регламенте должен быть описан порядок проведения экспертизы, критерии, ответственные	-	Осуществляется сотрудниками Заказчика после проведения обучения разработчиков	
Безопас-ное коди-рование	3.12.8	5.6 и 5.7	Исходный код	Разработка, уточнение и анализ архитектуры программного обеспечения, обеспечивающей снижение или исключение возникновения потенциальных уязвимостей	Архитектурные решения необходимо документировать и проводить их анализ	-	УЦСБ осуществляется ревью архитектурных изменений ПО и анализ соответствия требованиям к архитектуре	
Безопас-ное коди-рование	3.12.9	5.8	Исходный код	Формирование и поддержание в актуальном состоянии правил безопасного кодирования	Правила кодирования должны быть зафиксированы и доступны разработчикам	-	УЦСБ разрабатывает рекомендации по безопасному кодированию для используемых у Заказчика языков	
Безопас-ное коди-рование	3.12.10	5.9	Исходный код	Экспертиза исходного кода программного обеспечения	В регламенте должны быть описаны: порядок экспертизы, ответственные, периодичность	-	УЦСБ осуществляет разработку регламента проведения экспертизы исходного кода. Исполнитель осуществляет экспертизу исходного кода после каждого внесения изменений в соответствии с Регламентом безопасного кодирования	
Безопас-ное коди-рование	3.12.11	5.10	Исходный код	Проведение статического анализа кода	В регламенте должны быть описаны: порядок анализа, используемые инструменты, критерии прохождения	-	УЦСБ внедряет необходимые инструменты статического анализа, проводит первый полный разбор сработок и корректировку политик сканирования	Включено в Apsafe. УЦСБ осуществляет полный анализ исходного кода и далее — инкрементальный анализ изменений
Безопас-ное коди-рование	3.12.12	5.11	Исходный код	Проведение динамического анализа кода программ	В регламенте должны быть описаны: порядок анализа, используемые инструменты, критерии прохождения	-	УЦСБ внедряет необходимые инструменты динамического анализа, проводит первый полный разбор сработок и корректировку политик сканирования	Включено в Apsafe. УЦСБ осуществляет полный регулярный динамический анализ кода
3. Безопасность среды разработки								
Процесс разработки	3.12.13	5.12	Процесс разработки ПО	Использование безопасной системы сборки программного обеспечения	В регламенте должны быть описаны: порядок анализа, используемые инструменты, критерии прохождения	-	УЦСБ разрабатывает регламент безопасной сборки ПО, помогает изменить pipeline сборки для соответствия регламенту	
Процесс разработки	3.12.14	5.13	Процесс разработки ПО	Обеспечение безопасности сборочной среды программного обеспечения	Меры по защите сборочной среды должны быть описаны в регламенте	-	УЦСБ разрабатывает регламент безопасности сборочной среды и рекомендации по приведению текущей сборочной среды к целевому состоянию	
Процесс разработки	3.12.15	5.16	Исходный код	Проведение композиционного анализа программного обеспечения	В регламенте должны быть описаны: порядок анализа, инструменты, реагирование на уязвимости	-	УЦСБ внедряет необходимые инструменты композиционного анализа, проводит первый полный разбор сработок и корректировку политик сканирования	Включено в Apsafe. УЦСБ осуществляет полный анализ зависимостей и далее - инкрементальный анализ изменений
Процесс разработки	3.12.16	5.17	Исходный код	Проверка программного кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок его составных частей	Меры по проверке цепочек поставок (проверка цифровых подписей, поставщиков)	-	УЦСБ реализует практику подписания артефактов и доверенного репозитория, разрабатывает регламент	Доступ к безопасному репозиторию Apsafe, подписание артефактов, разработка регламента
4. Тестирование и выпуск								
Процесс разработки	3.12.17	5.18 и 5.19	Процесс раз+C19+D19	Функциональное и нефункциональное тестирование программного обеспечения	В регламенте должны быть описаны: порядок тестирования, виды тестов, критерии приемки	-	УЦСБ разрабатывает регламент тестирования ПО, Заказчик проводит функциональное тестирование, УЦСБ осуществляет консультации по достаточности тестов	
Процесс разработки	3.12.18	5.20	Процесс разработки ПО	Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения	Процедура выпуска (проверка подписей, сканирование, утверждение)	-	УЦСБ разрабатывает регламент выпуска готовой продукции	
Процесс разработки	3.12.19	5.21	Процесс разработки ПО	Безопасную доставка и установка программного обеспечения в информационных системах	Порядок доставки и установки, контроль целостности, использование защищенных каналов	-	УЦСБ разрабатывает регламент доставки готовой продукции	
5. Сопровождение и устранение уязвимостей								
Процесс разработки	3.12.20	5.22	Процесс разработки ПО	Обеспечение поддержки программного обеспечения при эксплуатации пользователями	В регламенте должен быть описан порядок взаимодействия при поддержке	-	УЦСБ разрабатывает регламент технической поддержки	
Процесс разработки	3.12.21	5.23	Процесс разработки ПО	Реагирование на информацию об уязвимостях программного обеспечения, поступающую от пользователей	Процедура реагирования (регистрация, анализ, устранение, уведомление)	-	УЦСБ разрабатывает регламент реагирования на уязвимости	
Процесс разработки	3.12.22	5.23	Процесс разработки ПО	Устранение уязвимостей программного обеспечения, выявленных в ходе его эксплуатации	Порядок устранения, приоритизация, тестирование исправлений	-	УЦСБ разрабатывает регламент устранения уязвимостей	
Процесс разработки	3.12.23	5.24	Процесс разработки ПО	Поиск уязвимостей в программном обеспечении и разработку мер по их устранению	В регламенте должен быть описаны: порядок поиска (пентесты, сканеры, внешние эксперты) и механизмы устранения	Поиск уязвимостей в программ-ном обеспечении в рамках открытых программ с привлече-нием внешних экспертов и разработка мер по их устранению	УЦСБ разрабатывает регламент регулярного анализа защищенности ПО	

При проверке документации подрядчика необходимо убедиться, что каждое требование зафиксировано в соответствующем регламенте или техническом задании. Отсутствие любого из них — основание для доработки документации.