КСБ-СОФТ

Создание и развитие цифровых продуктов на платформе ГосТех или как соответствовать требованиям по разработке безопасного ПО

Степан Харитонов
руководитель центр компетенций
по безопасной разработке

Александр Ванямов
руководитель регионального
направления

Обменивайтесь
сообщениями во вкладке «Чат»

Запись вебинара направим
всем участникам на указанный
при регистрации e-mail

Задавайте вопросы
во вкладке «Вопросы»

За лучший вопрос подарим
корпоративный мерч

План вебинара

- Актуальная проблематика
- Способы решения
- Кейсы
- Ответы на вопросы

Что такое разработка безопасного ПО (SSDLC)

SDLC (Software Development Lifecycle)

Жизненный цикл разработки ПО.
SDLC подразумевает действия и задачи, которые осуществляются в ходе разработки ПО.
В SDLC нет анализа безопасности разрабатываемого продукта.

SSDLC (Security Software Development Lifecycle)

Набор процедур безопасной разработки ПО, позволяющий обнаруживать и устранять уязвимости на ранней стадии, до публикации релиза продукта.

Почему стоит задуматься о внедрении безопасной разработки

28 000+

уязвимостей
обнаружили по итогам 2023 г.
(число растёт с каждым годом)

90%

инцидентов
безопасности вызваны
дефектами исходного кода

80%

веб-приложений
имеют хотя бы одну
опасную уязвимость

до 78%

доля
открытого исходного кода
в ПО в некоторых отраслях

21%

утечек данных
вызван уязвимостями
программного обеспечения

1 из 3

приложений
содержит
критическую уязвимость

SDL – не только про «безопасность», это один из доменов качественной разработки!

Для кого

Разработчики ПО в составе ГИС на платформе ГосТех

Дополнительные сервисы платформы

Базовые сервисы платформы

Сервисы ИБ

Инфраструктурные технологические сервисы (Гособлако)

Облачная платформа (ГосТех)

Аппаратное обеспечение

ЦОД

Сервисы взаимодействия с контейнером разработки

Шифрованные каналы связи

Сегмент привилегированных пользователей

Поставщики сервисов для платформы ГосТех

Нормативная база

Концепция разработки безопасного программного обеспечения на единой цифровой платформе Российской Федерации «ГосТех»

утверждена протоколом Президиума Правительственной комиссии от 04 мая 2023 г. № 20

Методические рекомендации «Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех». Основные требования к составу и функциями»

утверждены протоколом Президиума Правительственной комиссии от 05 августа 2022 г. № 30

Методические рекомендации по включению сервисов в Единую цифровую платформу Российской Федерации «ГосТех»

утверждены протоколом Президиума Правительственной комиссии от 05 августа 2022 г. № 30

Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы «ГосТех»

утверждены протоколом Президиума Правительственной комиссии от 08 декабря 2022 г. № 54

Меры по ГОСТ Р 56939-2016

Основные процессы	Этап 1 «Анализ требований»	1. Определение требований по безопасности
	Этап 2 «Проектирование архитектуры ПО»	2. Моделирование угроз 3. Уточнение проекта архитектуры ПО
	Этап 3 «Конструирование и комплексирование ПО»	4. Использование идентифицированных инструментальных средств разработки 5. Создание ПО на основе уточненного проекта архитектуры 6. Порядок оформления исходного кода 7. Статический анализ 8. Экспертиза исходного кода
	Этап 4 «Квалификационное тестирование ПО»	9. Функциональное тестирование 10. Тестирование на проникновение 11. Динамический анализ 12. Фаззинг-тестирование
Обеспечивающие процессы	Этап 5 «Инсталляция и приемка ПО»	13. Обеспечение целостности ПО в процессе передачи пользователю 14. Поставка пользователю эксплуатационных документов
	Этап 6 «Поддержка в процессе эксплуатации»	15. Процедуры отслеживания и исправления ошибок и уязвимостей ПО в ходе ЖЦ 16. Систематический поиск уязвимости
	Этап 7 «Менеджмент конфигурации»	17. Процедуры уникальной маркировки версий ПО 18. Использование системы управления конфигурацией ПО
	Этап 8 «Менеджмент среды разработки»	19. Защита от НСД к элементам конфигурации 20. Резервное копирование 21. Регистрация событий, связанных изменения элементов конфигурации
	Этап 9 «Менеджмент персонала»	22. Периодическое обучение сотрудников и анализ программы обучения

Меры по Методическим рекомендациям по обеспечению безопасности при разработке ПО с использованием платформы «ГосТех»

Основные процессы	Этап 1 «Анализ и формирование требований к разрабатываемому ПО»	1. Разработка требований по безопасности **2. Моделирование угроз безопасности информации**
	Этап 2 «Конструирование и комплексирование ПО»	**3. Уточнение проекта архитектуры ПО** 3. Идентификация инструментальных средств разработки ПО 4. Создание программы на основе уточненного проекта архитектуры программы 5. Порядок оформления исходного кода программы 6. Статический анализ исходного кода программы 7. Экспертиза исходного кода программы
	Этап 3 «Квалификационное тестирование ПО»	8. Функциональное тестирование программы 9. Фаззинг-тестирование программы 10. Динамический анализ программы 11. Тестирование на проникновение
Обеспечивающие процессы	Этап 4 «Инсталляция программы и поддержка приемки ПО»	12. Обеспечение защиты ПО в процессе его передачи Заказчику 13. Поставка Заказчику эксплуатационных документов
	Этап 5 «Решение проблем в процессе эксплуатации»	14. Отслеживание и исправление обнаруженных недостатков программы и уязвимостей 15. Систематический поиск уязвимостей программы
	Этап 6 «Управление документацией и конфигурацией программы»	16. Уникальная маркировка каждой версии ПО 17. Использование системы управления конфигурацией
	Этап 7 «Управление инфраструктурой среды разработки ПО»	18. Защита от НСД к элементам конфигурации 19. Резервное копирование 20. Регистрация событий, связанных с фактами изменения элементов конфигурации
	Этап 8 «Обучение работников и периодический анализ программы обучения»	21. Периодическое обучение сотрудников и анализ программы обучения

Рекомендованные требования по безопасности к разрабатываемому ПО в составе ГИС на платформе «ГосТех»

Требования по безопасности

- Этап 1 «Требования к архитектуре, дизайну и моделированию угроз»
- Этап 2 «Требования к аутентификации»
- Этап 3 «Требования к управлению сессиями (Session Management)»
- Этап 4 «Требования к контролю доступа»
- Этап 5 «Требования к валидации, очистке и кодированию»
- Этап 6 «Требования к обработке ошибок и ведению журнала»
- Этап 7 «Требования к защите данных»
- Этап 8 «Требования к каналам связи»
- Этап 9 «Требования к защите от вредоносного воздействия»
- Этап 10 «Требования к бизнес-логике»
- Этап 11 «Требования к файлам и ресурсам»
- Этап 12 «Требования к API и веб-сервисам»
- Этап 13 «Требования к конфигурации»

1. Требования к архитектуре и моделированию угроз

1.1. Требования к жизненному циклу безопасной разработки ПО

№	Описание	К3	К2	К1
1.1.1	Безопасность должна обеспечиваться на всех этапах жизненного цикла разработки ПО		x	x
1.1.2	Для каждого изменения архитектуры программы должно осуществляться моделирование угроз, планирование компенсирующих мер, вариантов реагирования на угрозы и разработка алгоритмов тестирования запланированных мер	x	x	x
1.1.3	Все пользовательские функции выполняют необходимые требования безопасности (разграничение действий по чтению, записи и исполнению)		x	x
1.1.4	Разработка документации с обоснованием всех границ доверия, ролевой модели доступа и фиксации событий аудита программы, ее компонентов и всех значимых потоков данных		x	x
1.1.5	Анализ безопасности высокоуровневой архитектуры программы и всех подключаемых удалённых служб		x	x
1.1.6	Реализация централизованных, надежных и переиспользуемых функций безопасности, разработанных с применением мер по разработке ПО		x	x
1.1.7	Наличие перечня обязательных требований по безопасному программированию, требований безопасности к разрабатываемому ПО, рекомендаций или политик для всех разработчиков и тестировщиков		x	x

Поставщики цифровых продуктов на платформе ГосТех

Какие цифровые продукты можно предложить

В каталог цифровых продуктов можно добавить:

Собственные отраслевые решения

Готовые к использованию программные продукты, обеспечивающие цифровизацию специфических отраслевых задач

Решения, расширяющие возможности базовых сервисов

В каталог цифровых продуктов могут быть включены решения, поставляемые как:

- Дистрибутивы
- Облачные решения

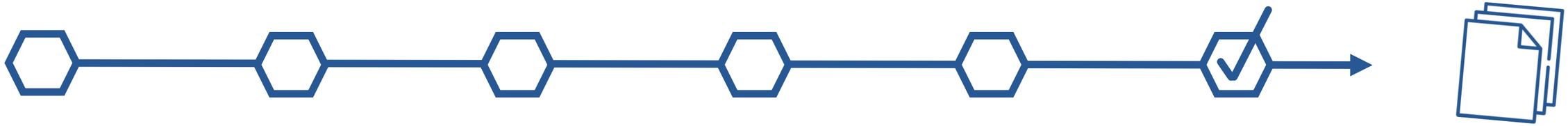
Кто может стать поставщиком цифровых продуктов

Отечественная организация, ИП, физическое лицо, которые:

- соответствуют требованиям к участникам закупок в соответствии с 44-ФЗ
- обладают правами на цифровой продукт
- применяют стандарты разработки безопасного ПО

https://platform.gov.ru/postavshikam/

Как подать заявку на включение в каталог цифровых продуктов



Подготовка

Направление заявления

Проверка заявления

Технические испытания

Утверждение решения

Внесение в каталог

https://platform.gov.ru/postavshikam/

Как подать заявку на включение в каталог цифровых продуктов

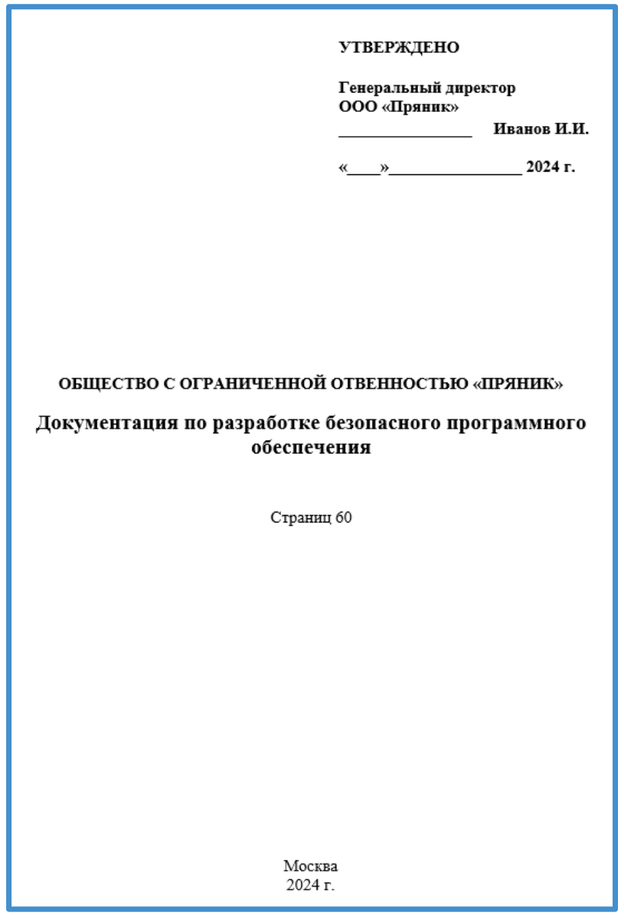
Этап «Подготовка»

- Знакомство с требованиями платформы ГосТех
- Описание схемы развертывания продукта на платформе ГосТех (дистрибутив, Docker, Kubernetes)
- Подготовка описания архитектуры, опишите предполагаемый способ интеграции своего решения с базовыми сервисами платформы ГосТех.

  Обязательна интеграция с базовыми сервисами платформы:
  - *управление пользователями (IAM)*
  - *журналирование*
  - *аудит*
  - *мониторинг (ЖАМ)*
- Определите индикативные тарифы предоставления продукта заказчикам.

  Целевая модель тарификации — оплата исходя из фактического объема использования цифрового продукта (по количеству пользователей, по объему задействованной инфраструктуры).
- Если продукт не сертифицирован ФСТЭК России:
  - внедрите в компании процессы разработки безопасного ПО в соответствии с ГОСТ Р 56939-2016
  - самостоятельно или с помощью привлеченной лаборатории проведите для цифрового продукта анализ уязвимостей в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013
  - используйте для идентификации и авторизации пользователей базовый сервис IAM
- Актуализируйте документацию, включая описание процедур обеспечения надежности, руководство пользователя, руководство по установке, описание внешних зависимостей, методику расчета требуемых вычислительных ресурсов.
- Определите, какие функции продукта являются ключевыми для включения их в программу и методику испытаний (ПМИ).

Свидетельства о процессах разработки безопасного ПО



УТВЕРЖДЕНО

Генеральный директор
ООО «Пряник»
_____ Иванов И.И.

«____»_____ 2024 г.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕННОСТЬЮ «ПРЯНИК»

Документация по разработке безопасного программного обеспечения

Страниц 60

Москва
2024 г.

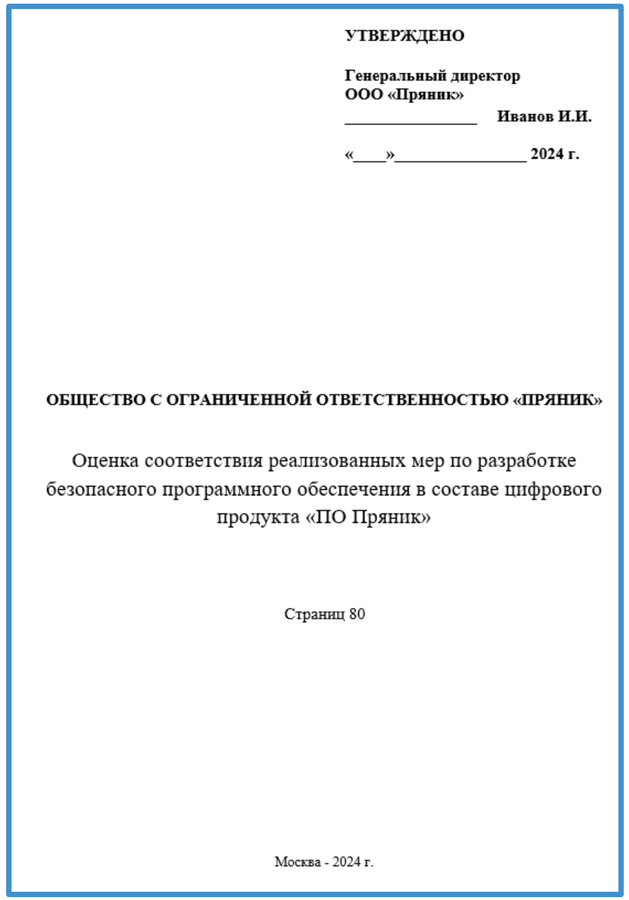
Содержит документацию по разработке безопасного программного обеспечения принятые в организации.

Процессы, описанные в нем, направлены на **обеспечение необходимого уровня защиты информации**, посредством реализации мер, минимизирующих количество уязвимостей и недостатков программ на всех этапах жизненного цикла ПО и ведутся с использованием мер ГОСТ Р 56939-2016.

Содержит следующие основные сведения:

- какие меры РБПО реализуются на каждом этапе ЖЦ разработки продукта?
- кем обеспечиваются меры РБПО?
- какие мероприятия должны быть выполнены по результатам успешной реализации мер РБПО?

Свидетельства о процессах разработки безопасного ПО



УТВЕРЖДЕНО

Генеральный директор
ООО «Пряник»
_____ Иванов И.И.

«____»_____ 2024 г.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПРЯНИК»

Оценка соответствия реализованных мер по разработке безопасного программного обеспечения в составе цифрового продукта «ПО Пряник»

Страниц 80

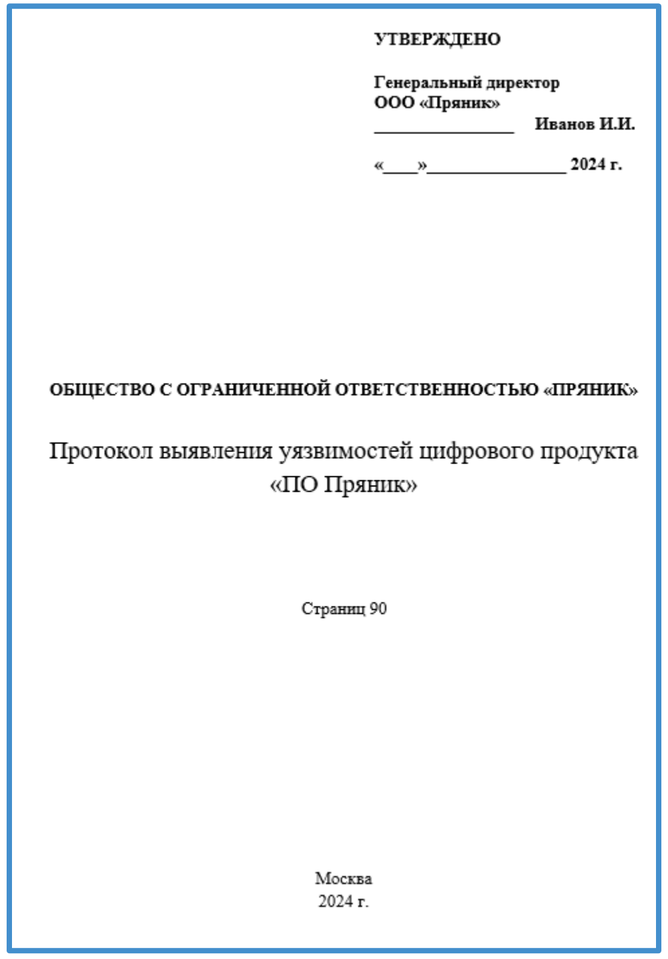
Москва - 2024 г.

Содержит **оценку** соответствия **реализованных мер** по разработке безопасного программного обеспечения с приложением результатов проведенных испытаний по выявлению уязвимостей в программном обеспечении цифрового продукта.

В качестве оценки соответствия для цифрового продукта предоставляются:

- описание реализации процесса разработки безопасного программного обеспечения разработчиком в соответствии с требованиями ГОСТ Р 56939-2016;
- результаты проведенных испытаний по выявлению уязвимостей в программном обеспечении цифрового продукта.

Свидетельства о процессах разработки безопасного ПО



УТВЕРЖДЕНО

Генеральный директор
ООО «Пряник»
_____ Иванов И.И.

«____»_____ 2024 г.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПРЯНИК»

Протокол выявления уязвимостей цифрового продукта «ПО Пряник»

Страниц 90

Москва
2024 г.

Исследование проводится с целью выявления уязвимостей, условий и факторов, создающих возможность нарушения целостности объекта оценки, а также нарушения конфиденциальности, целостности и доступности обрабатываемой (защищаемой) информации в цифровом продукте.

Что содержит:

- условия проведений испытаний;
- ограничения на проведение испытаний;
- оцениваемые характеристики;
- учитываемые возможности нарушителя;
- результаты проведенных испытаний с приложением выходных артефактов.

Центр экспертизы по безопасной разработке КСБ-СОФТ

01 Внедрение и развитие процессов безопасной разработки

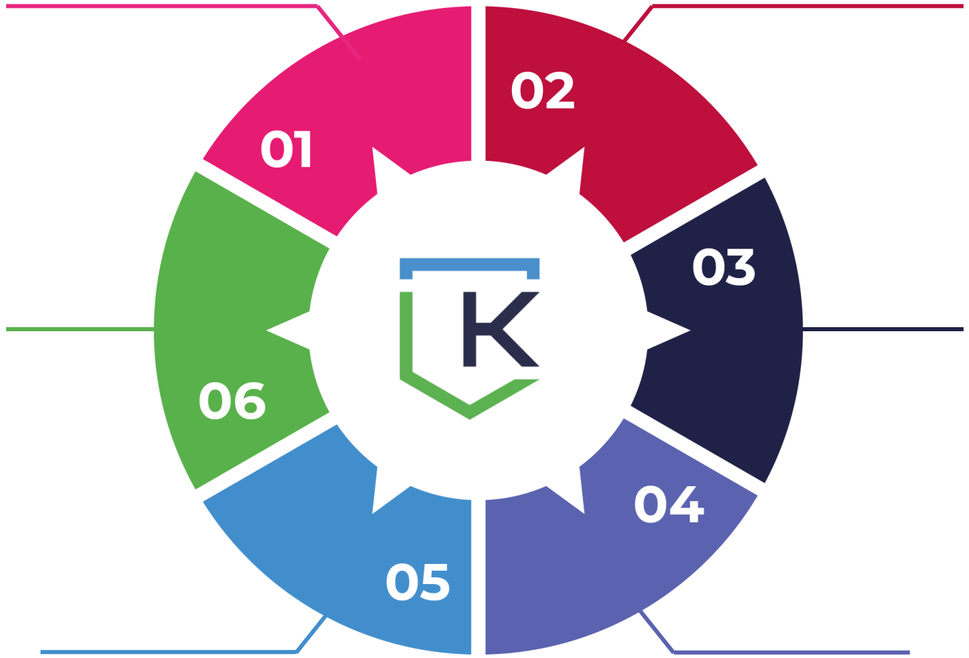
02 Разработка документации, описывающую разработку безопасного программного обеспечения

03 Проверка соответствия требованиям стандартов

04 Проведение аудита процессов (безопасной) разработки

05 Обеспечение безопасности приложений во время их выполнения

06 Проведение композиционного, статического и динамического анализа, функционального и фаззинг-тестирования



«КСБ-СОФТ»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Команда специалистов ИБ и инженеров

80+ регионов внедрения

4000+ реализованных проектов

Лицензиат ФСТЭК России

Лицензиат ФСБ России

ПРОМО-ПРЕДЛОЖЕНИЕ

Композиционный анализ ПО за 1 день
по фиксированной цене!

- подключение к вашему VCS (не более 1 VCS)
- анализ 1 репозитория внутри VCS
- проверка Open Source и обнаружение Open Source зависимостей
- предоставление и разбор информации о найденных уязвимостях и лицензиях
- построение графов связей компонентов
- формирование реестра компонентных связей SBoM
- отчет о наличии уязвимых компонентов (не более 1 отчета)

Заполните опросный лист!

Сделайте первый шаг к новому видению информационной безопасности вместе с нами!

ksb-soft.ru

+7 (8352) 322-322

info@ksb-soft.ru

Телеграм-канал «Мнение интегратора»

Закрытое SDL-коммьюнити