

Процесс 21. Безопасная поставка программного обеспечения пользователям





Александр Гадай,
руководитель службы консалтинга

✉ agadai@swordfishsecurity.ru
📌 [@a_gadai](#)



Мария Рачёва,
ведущий аналитик процессов
безопасной разработки

✉ mracheva@swordfishsecurity.ru
📌 [@rachevamarina](#)

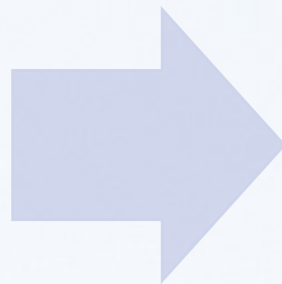
Взгляд на безопасную поставку ПО со стороны ГОСТ 56939 - 2024:

Цель

Обеспечить защиту ПО при поставке до конечного пользователя

Требования

- Фиксация версий ПО, в том числе эксплуатационной документации;
- Организация централизованного и защищенного хранения копий ПО и документации.



Артефакты

- Регламент безопасной поставки ПО;
- Эксплуатационная документация на ПО;
- Автоматизированный учет версий ПО (система контроля версий);
- Защищенное место хранения копий ПО и документации с реализации механизма проверки целостности;
- Реализация условий для проведения проверки целостности на стороне конечного пользователя.

Как фиксировать версию ПО:



**Использовать систему контроля версий,
развернутую внутри контура вашей
Организации**

- Фиксировать актуальную версию поставляемого ПО в репозитории Системы контроля версий Организации
- Фиксировать актуальную версию поставляемого ПО в составе эксплуатационной документации.
- Сведения о версии необходимо фиксировать в электронном виде или на физическом носителе

Что входит в состав эксплуатационной документации на ПО:



Поставка ПО должна проводиться с комплектом эксплуатационной документации, с описанием:

- Версии поставляемого ПО
- Сведений о месте хранения копий (подлинников, дубликатов) версий ПО (инсталляционных пакетов, дистрибутивных носителей)
- Штатного функционирования ПО
- Параметров настроек (конфигураций) ПО
- Параметров среды функционирования ПО
- Действий по установке и настройке ПО как с точки зрения функционала, так и безопасности

Что входит в состав Регламента безопасной поставки ПО:



Регламент должен описывать «реальный» процесс, а не формальный подход, и определять:

- ➔ Обязанности работников и их роли при реализации процесса безопасной поставки ПО
- ➔ Способ и место хранения версий поставляемого ПО в защищенном виде
- ➔ Способ снятия копий поставляемого ПО, а также хранения копий в защищенном виде
- ➔ Порядок реализации процесса безопасной поставки ПО, в том числе обновлений ПО
- ➔ Процедуру создания условий для проверки подлинности ПО (обновлений ПО)
на стороне пользователя

Как правильнее показать распределение ответственности участников процесса:



Нагляднее всего показывать зоны ответственности в следующем виде – Матрица RACI:

Группы	Группа 1		Группа 2				Группа 3		
Роли	Роль 1	Роль 2	Роль 3	Роль 4	Роль 5	Роль 6	Роль 7	Роль 8	Роль 9
Задачи									
Задача 1	A R	C			I			I	C
Задача 2	C	C			I			A	R
Задача 3			R						

Responsible (R)	Непосредственный исполнитель Несет ответственность за выполнение работы
Accountable (A)	Руководитель Отвечает за конечный результат Координирует задачи и ведет контроль за работой исполнителей
Consult (C)	Эксперт по направлению Предоставляет необходимую информацию
Inform (I)	Информируется о результатах выполненных работ для дальнейшего использования по процессу и аналитики Получает информацию о результате на шаге выхода задачи

Порядок реализации процесса:

Внедрение системы контроля версий и хранения артефактов



Внедрение механизмов контроля целостности



Разработка и внедрение процесса и закрепление его
Регламентом безопасной поставки ПО



Назначение ответственных исполнителей



Назначение ответственных за контроль исполнения
требований

Определение уровня реализации

ГОСТ определяет требований к реализации процесса



Проведение оценки соответствия требования ГОСТа
показывает Уровень реализации процесса



Уровни реализации можно разложить по трехуровневой градации от
минимального набора до максимальной реализации

На что стоит обращать внимание



- 1** Разработка ОРД и построение процесса не «для галочки»
- 2** Внедрение только инструментов это «половина результата»
- 3** Минимальный подход = минимальный уровень реализации

С чего лучше начинать



1

Аудит процессов разработки

2

Определение текущего уровня реализации процессов РБПО

3

Разработка Плана реализации процессов для достижения необходимого уровня

Спасибо за внимание!

SWORDFISH
SECURITY

📍 Москва, Береговой пр-д, д. 5, к. 1, БЦ Волна
+7 (495) 620-63-36

✉ info@swordfish-security.ru



swordfish-security.ru



Мы в Telegram



Мы на Хабре

