ИСП РАН

О сертификации процессов РБПО

ПАДАРЯН В.А.
vartan@ispras.ru
Заведующий лабораторией ИСП РАН

08 октября 2024

ITSEC 2024

Разработка безопасного ПО (РБПО)
Нормативная база

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 3 апреля 2018 г. N 55

ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ
О СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 2 июня 2020 г. № 76

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

(издание второе, доработанное)

П Р И К А З

21 декабря 2017 г. Москва № 235

Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

П Р И К А З

25 декабря 2017 г. Москва № 239

Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

УТВЕРЖДЕН
приказом ФСТЭК России
от 1 декабря 2023 г. № 240

Зарегистрирован Минюстом России
16 апреля 2024 г. № 77896

Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации

Национальные стандарты в области разработки безопасного ПО

Зачем сертификация и что она дает

- Любое ПО требует выпуска обновлений безопасности, сертифицированное ПО – не исключение
  - Огромный объем кода, использование OSS компонент, …
- Задача: сохранив безопасность ПО, снизить издержки разработчиков, ускорить доставку обновлений пользователям

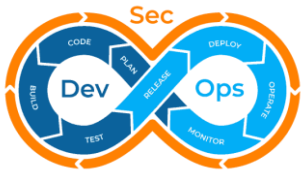
- Приказ ФСТЭК России №55
  71.1. Заявитель, являющийся разработчиком СЗИ и имеющий сертификат соответствия процедур безопасной разработки ПО требованиям национальных стандартов в области ЗИ, в случае внесения в сертифицированное средство защиты информации изменений <…> проводит испытания средства защиты информации самостоятельно
- Предполагается, что с 25 года самостоятельно вносить изменения в сертифицированное ПО смогут только сертифицированные компании
  - Возможность оперативно выпускать обновления безопасности
  - Комплект материалов для обновленного ПО в уведомительном порядке направляется во ФСТЭК России

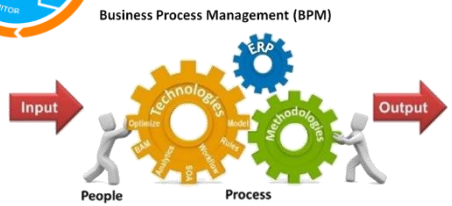
Что сертификация **не позволяет**

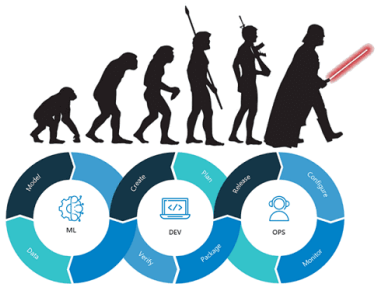
- Считать сертифицированным все ПО, которое разрабатывается на сертифицированном «сборочном конвейере»
- Самостоятельно выполнять функции испытательной лаборатории при первичной сертификации программного продукта
- Возможность самостоятельно готовить обновления сертифицированного ПО при существенном изменении ПО – в «серой зоне»
  - После изменения архитектуры и/или большей части кодовой базы можно ли считать, что это все еще то ПО, которое проходило сертификацию с участием ИЛ

Ожидания vs. Реальность

- 24 мая 2024 года ИСП РАН стал аккредитованным органом по сертификации в 5 области
- Какие компетенции требуются от специалистов органа по сертификации процессов РБПО?
  - Понимание, как на самом деле работают инструменты анализа кода DevOps, DevSecOps, AppSec, SAST/DAST, Fuzzing, Pentest, VCS, …
  - Опыт внедрения SDL/РБПО в крупных зарубежных (а теперь – и отечественных) компаниях
  - Здравый смысл
- Команда профильных экспертов из разных отделов Института



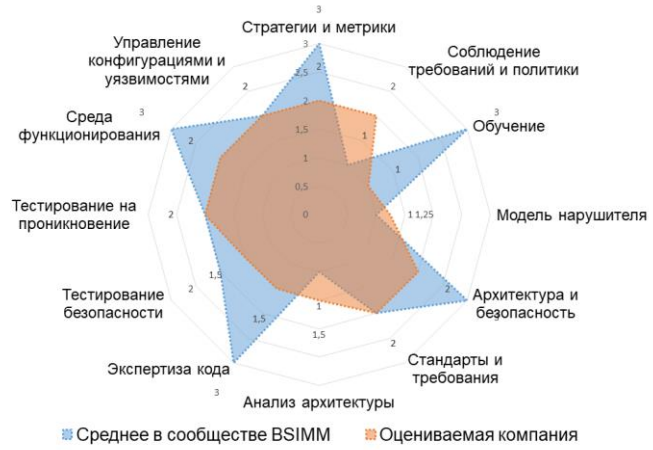




- Изучается плотный кисель бизнес процессов, куда все в части РБПО должно органично входить и жить в симбиозе
  - Система РБПО строится и отлаживается годами, а изучить ее надо за считанные дни
- Много корпоративного сленга
- POV разработчика
  - Аудитор ≡ Противник
- Чем строже в компании ИБ, тем сложнее получать требуемую информацию

Оценка процессов РБПО – мировой опыт

BSIMM



OWASP SAMM

- Оценивание по независимым аспектам
- Уровни зрелости – «вкусовой» вопрос
  - Несоответствие требованиям, начальный уровень, базовый, базовый усиленный, продвинутый
- Необходимо учитывать реалии внедрения РБПО в РФ
  - Только СЗИ или все ИТ-вовлеченные отрасли?

Методология оценки соответствия

На что и как смотрим?

- Порядок оценки временный, до вступления в действие ГОСТ Р 56939-2024
- По результатам проведенной сертификации готовятся заключение и протокол
- Сертификат соответствия выдается организации-заявителю на срок, указанный в заявке, но не более, чем на пять лет (Приказ №240)
- В сертификате указывается соответствие стандарту ГОСТ Р 56939-2016
  - Протокол содержит расширенную информацию
    - На примере каких программных продуктов оценивается соответствие Требуется показать реализацию процессов для более чем одного программного продукта
    - Описываются процессы разработки в организации, включая применяемые автоматизированные системы
    - Дается оценка соответствия требованиям ГОСТ Р 56939-2016 **и иных действующих стандартов** в области разработки безопасного ПО, например, ГОСТ Р 71207-2024


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71207— 2024

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Статический анализ программного обеспечения. Общие требования

Издание официальное

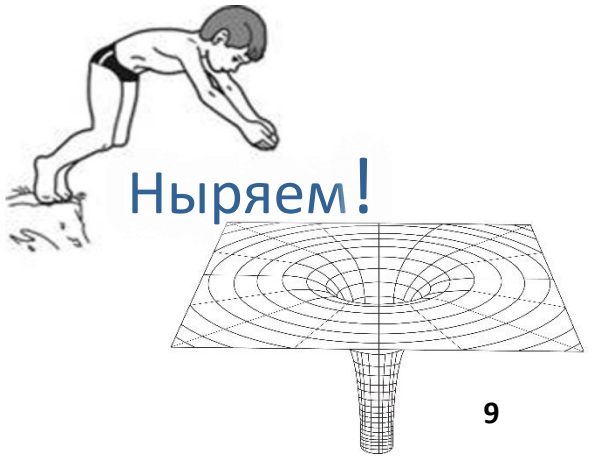
Москва
Российский институт стандартизации
2024

- Изучаются не только документы, но и практическая реализация процессов, их кадровое и техническое обеспечение
  - Руководство по разработке безопасного ПО – документ-«зонтик», утверждается руководством компании, содержит отсылки на регламенты отдельных мер/процессов
  - Инструментальный контроль отдельных аспектов сертифицируемых процессов

Кто участвует в сертификации (со стороны органа)

- Проектная команда
- Команда общей ИБ
- Команда DevOps
- Команда статического анализа и инструментов системы сборки
- Команда динамического анализа и фаззинг-тестирования
- Команда функционального тестирования
- Итого: команда 10+ экспертов

- Этапы работы
  - Подготовительный
  - Знакомство с командами разработчиков
  - Интенсив по мерам/процессам
  - Подготовка протокола



Пример: оценка процесса статического анализа (ГОСТ Р 71207-2024)

- …
- В целях своевременного выявления и исправления ошибок статический анализ должен регулярно применяться к разрабатываемому ПО. <…> Статический анализ всего разрабатываемого ПО целиком следует выполнять не реже одного раза в десять рабочих дней, если за данный период времени исходный код был изменен.
- Результаты каждого проведенного статического анализа должны сохраняться в хранилище результатов анализа.
- В случае использования при разработке ПО системы непрерывной интеграции проведение статического анализа должно быть включено в состав автоматически выполняемых проверок кода.
- <…> В целях своевременной и эффективной работы с полученными результатами статического анализа просмотр выданных анализатором предупреждений следует выполнять:
  - в случае анализа измененных частей ПО – не позже, чем через три рабочих дня после выполнения анализа;
  - в случае анализа ПО целиком – не позже, чем через десять рабочих дней после выполнения анализа.
- Конфигурация и настройки статического анализатора должны регулярно пересматриваться
- …

Buildography — инструмент для идентификации реквизитов сборки

- Реквизиты сборки
  - Файлы с исходным кодом и зависимости (системные библиотеки, заголовочные файлы и т.п.)
  - Трансляторы и их конфигурационных файлы
- Результат — структурированная информация о выполнении сценария сборки ПО
- Buildography отслеживает системные вызовы дочернего дерева процессов с помощью системного вызова ptrace

```
{
    "directory": "/root",
    "input": { "/root/main.c": "..." },
    "commands": [ "gcc", "main.c" ],
    "component_commands": [
        {
            "command": [ "/usr/lib/gcc/x86_64-linux-gnu/11/cc1", "...", ],
            "dependencies": { "/etc/ld.so.cache": "...", },
            "output": { "/tmp/ccUEQNfb.s": "..." }
        },
        ...
    ],
    "utilities": [ { "path": "/usr/bin/x86_64-linux-gnu-gcc-11", "hash": "..." }, ... ]
}
```

Можно сейчас ли подводить первые итоги?

- Для каждого производителя его решение РБПО самое лучшее, но требования ГОСТ должны выполняться.
  - Работа сертификатора РБПО – оценить, выполняются требования совокупностью реализованных процессов
- Завершена сертификация Лаборатории Касперского, ведется сертификация Сбербанк-Технологии
- Очередь на сертификацию процессов РБПО сформирована до конца 2025 года
- У крупных вендоров относительно хорошо внедрен ГОСТ Р 56393-**2016**
  - ГОСТ Р 56939-2024 добавляет новые требования

ГОСТ Р 56939-2024

Сквозные процессы	№01 Планирование процессов разработки безопасного программного обеспечения NEW
	№02 Обучение сотрудников
Проектные процессы	**№03 Формирование и предъявление требований безопасности к программному обеспечению**
Анализ и трансформация программ: технологические требования	№04 Управление конфигурацией программного обеспечения
	№05 Управление недостатками и запросами на изменение программного обеспечения
	№06 Разработка, уточнение и анализ архитектуры программного обеспечения
	№07 Моделирование угроз и разработка описания поверхности атаки
	№08 Формирование и поддержание в актуальном состоянии правил кодирования
	№09 Экспертиза исходного кода
	№10 Статический анализ исходного кода
	№11 Динамический анализ кода программы
	№12 Использование безопасной системы сборки программного обеспечения
	№13 Обеспечение безопасности сборочной среды программного обеспечения
	№14 Обеспечение управления доступом и целостности кода при разработке программного обеспечения
	№15 Обеспечение безопасности используемых секретов
	№16 Использование инструментов композиционного анализа
	№17 Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок NEW
	№18 Функциональное тестирование
	№19 Нефункциональное тестирование
	№20 Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения
	№21 Безопасная поставка программного обеспечения пользователям
	№22 Обеспечение поддержки программного обеспечения на этапе эксплуатации пользователями
	№23 Обеспечение реагирования на информацию об уязвимостях
	№24 Поиск уязвимостей в программном обеспечении при эксплуатации
	№25 Обеспечение безопасности при выводе программного обеспечения из эксплуатации NEW

Что будет дальше?

- После вступления в силу ГОСТ Р 56939-2024 ждем обновления приказа №240
- С 19 сентября РГ5 ТК362 начала работу над ГОСТ «Методика оценки уровня реализации процессов разработки безопасного программного обеспечения».
  - Первая редакция ожидается в декабре-январе
- На конференции ISP RAS OPEN (12-13 декабря) https://www.isprasopen.ru/ запланирован круглый стол, на котором планируется собрать первые 5 организаций, прошедшие сертификацию