Построение и автоматизация безопасной разработки в текущих реалиях: опыт заказчиков

Константин Саматов, член Правления Ассоциации руководителей служб информационной безопасности

Основные тренды

- ускорение разработки и внедрения отечественного ПО;
- потеря доверия к зарубежному и свободно-распространяемому ПО;
- с 01.01.2023 требования по безопасной разработке в ЗОКИИ
- с 01.01.2025 запрет на применение зарубежного ПО на ЗОКИИ (ОКИИ), ОГВ и компаниям с госучастием;
- с 01.01.2025 ОГВ и подавляющему большинству организаций запрещено использовать средства защиты информации из недружественных стран;
- дефицит кадров соответствующей квалификации.

Субъекты безопасной разработки

Разработчики (производители) программного обеспечения

Заказчики разрабатывающие ПО для собственных нужд

Заказчики использующие готовое ПО

Люди

Security Champion

VS

Security Officer

Процессы/требования

Формирование потребности

Формирование основных требований по ИБ

Проектирование

- Формирование перечня рисков
- Разработка модели угроз
- Формирование требований на основе рисков и модели угроз
- Включение требований в техническое задание
- Отражение требований в рамках технического проекта

Разработка

- Анализ уязвимостей архитектуры
- SAST
- DAST
- Fuzzing

Ввод в эксплуатацию

- Анализ уязвимостей ПО
- Тестирование на проникновение

Сопровождение

- Тестирование ПО на наличие уязвимостей
- Мониторинг уязвимостей в используемых библиотеках
- Устранение уязвимостей

Вывод из эксплуатации |модернизация\ доработка\ модификация

Контроль вывода из эксплуатации | начало цикла

Процессы/требования

1

Требования Банка России: 382-П, 683-П, 684-П, 719-П:

- Анализ и устранение уязвимостей ПО
- Соответствие ОУД или сертификация

2

П. 11 Состава и содержания… (21 Пр. ФСТЭК России). В случае определения в соответствии с Требованиями к защите ПДн (ПП №1119), в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно **могут применяться** следующие меры:

- проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
- тестирование информационной системы на проникновения;
- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Процессы/требования

3

Требования к владельцам ЗОКИИ. С 01.01.2023 дополняются п. 29.3 - 29.4 (Приказ ФСТЭК России от 20.02.2020 № 35):

29.3. Прикладное ПО, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) ЗОКИИ должно соответствовать:

- требованиям по безопасной разработке: наличие руководства по безопасной разработке программного обеспечения, проведение анализа угроз безопасности информации программного обеспечения, наличие описания структуры программного обеспечения на уровне подсистем;
- требованиям к испытаниям по выявлению уязвимостей в программном обеспечении: SAST, DAST, Fuzzing
- требованиям к поддержке безопасности программного обеспечения: отслеживание и исправление ошибок и уязвимостей, доведение разработчиком информации до его пользователей об уязвимостях и способах получения обновлений, окончании производства и/или поддержки ПО.

Процессы/требования

29.4. Выполнение требований 29.3 оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции, ремонту) или обеспечению безопасности ЗОКИИ, на этапе проектирования на основе документации разработчика ПО.

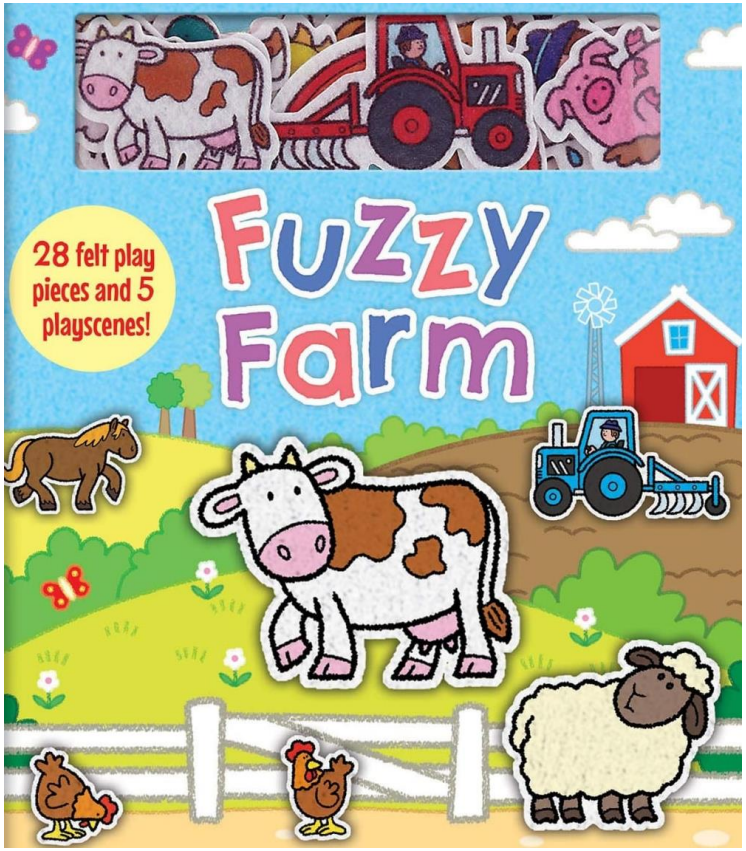
«Представитель ФСТЭК России добавил к этому, что предполагается, что
доказывать безопасность продукта **должны не компании, а разработчики**,
которые создали решение для организации. Альтернативные варианты
исполнения требований – привлечение стороннего аудита для проверки
систем или самостоятельная проверка и добровольная сертификация ~~по ГОСТу~~».

Источник: https://www.digital-energy.ru/wp-content/uploads/2022/04/По_итогам_встречи_с_регуляторами_16_03.pdf

Автоматизация процесса безопасной разработки

Статический анализ:

- есть отечественные качественные инструменты;
- ограничения на использование зарубежных анализаторов;
- не все языки программирования поддерживаются;
- необходимость ручной обработки результатов: большой объем, наличие специалиста



Динамический анализ:

- отсутствие комплексных решений (есть наборы утилит, зарубежных);
- необходимость иметь полигон/полигоны/ фаззинг кластер (ферма).

Спасибо за внимание!

Константин Саматов, член Правления Ассоциации руководителей служб информационной безопасности