Безопасная разработка и Сертификация. Две стороны одной медали

Версия 2

Дмитрий Пономарев
ООО НТЦ «Фобос-НТ» / ИСП РАН
(@DmitryJustDmitry)

1.1. Актуальность безопасной разработки. Стратегия

Напряженная политическая обстановка. Нарастание информационного, технологического, экономического и пр. давления со стороны ряда государств. Ограничение доступа к технологиям, повышенные риски кибератак, в том числе уровня APT-группировок.

Комплексная угроза -> Комплексная защита:

1. Триумвират «Образование, Разработка, Инновации».

2. Принцип эшелонированной обороны:
   - физическая и административная защита;
   - привлечение SOC для выявления нестандартных и APT- угроз;
   - межсетевое экранирование, обнаружение вредоносной активности;
   - формирование политик организации и контроль за журналами;
   - проектирование и разработка приложений в парадигме безопасной разработки.

Собственная защищенность программного комплекса – последний рубеж обороны!

1.2. Актуальность безопасной разработки. Требования ФСТЭК России

Приказ №76 «Требования по безопасности информации…», раздел IV, п. 17.

Тестирование, испытания по выявлению уязвимостей и недекларированных возможностей, а также анализ скрытых каналов **проводятся изготовителем в ходе приемочных испытаний средства** и испытательной лабораторией в ходе сертификационных испытаний средства.

Приказ №121 «О внесении изменений в положение о системе сертификации…», п. 12.

При проверке организации производства программных и программно-технических средств защиты информации проверяется внедрение заявителем процедур безопасной разработки программного обеспечения **в соответствии с требованиями по безопасности информации, на соответствие которым проводятся сертификационные испытания**.

а также (*первоисточник уточните у представителя вашей ИЛ*):

«… если по совокупности выполнения пунктов «а» - «д» дана положительная оценка, **исследования ограничиваются верификацией результатов, предоставленных разработчиком**...».

1.3. Актуальность безопасной разработки. Неформально говоря

- парадигма: «отдадим собранный полгода назад комплекс бинарников в испытательную лабораторию, она нам что-то пофаззит, и можно считать испытания пройденными»;
  больше **системно** не работает!

- в настоящий момент требования к количественным и качественным характеристикам SDL- и сертификационных процессов задаются Положением о системе сертификации, Требованиями доверия и Методикой ВУ и НДВ. ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения» носит рекомендательный характер;

- безопасная разработка != «возьмём пару open-source анализаторов для видимости проведения исследований и оформим отчет с 200 000-ю формулировок «*Не эксплуатируемо, потому что не эксплуатируемо*»»:

- безопасная разработка == перманентный процесс, включающий выделенных сотрудников, технику, программные средства (**платные** и бесплатные) и понимание необходимости всего этого сотрудниками компании, от «джуна» до собственника.

Поставленный процесс – залог своевременного получения Сертификата соответствия и конкурентное преимущество XXI века!

2.1. Сертификация. Друзья и партнеры

- проводим аудит SDL-процессов в АО «Лаборатория Касперского» с тех пор, когда это ещё не было мейнстримом (в течение последних 5 лет):

- помогаем в улучшении SDL-процессов и сертификации компаниям:

  ООО «Айдеко», АО «Аладдин Р.Д.», АО «АМГ БР», ООО «Амикон», ООО «А-Реал Консалтинг», ООО «Базальт СПО», ООО «БеллСофт», ООО «BI.ZONE», ООО «Доктор Веб», ООО «Group-IB», ООО «Газинформсервис», ООО «Гарда Технологии», АО «ИВК», АО «Русатом Автоматизированные системы управления», ЗАО «Институт Сетевых Технологий», ООО «Код Безопасности», ООО «НПЦ КСБ», АО «Лаборатория Касперского», ООО «Нума Технологии», ООО «Постгрес Профессиональный», ООО «R-Vision», ООО «Secret Technologies», ООО «ТСС», ООО «Cyberpeak» и другим…

- участвовали в пилотных испытаниях по новым требованиям и методикам ФСТЭК России совместно с ИСП РАН, ООО «Код Безопасности» и АО «Лаборатория Касперского» в 2019 году;

- участвуем в подготовке и проведении образовательных курсов ФАУ "ГНИИИ ПТЗИ ФСТЭК России“ на базе ИСП РАН;

- принимаем активное участие в «пилотировании» методик и средств анализа, разработанных ИСП РАН и в развитии сообщества Центра компетенций под эгидой ФСТЭК России и ИСП РАН.

2.2. Сертификация. Практики безопасной разработки

Требуемые практики безопасной разработки (**выборочно**):

- моделирование и проектирование безопасной архитектуры;
- анализ безызбыточности внешних интерфейсов и прав доступа к ресурсам;
- статический анализа исходного кода;
- статический анализа конфигураций модулей и контейнеров;
- использование безопасных тулчейнов (компиляторы, линковщики и их параметры);
- использование безопасных сторонних и заимствованных компонентов (**в том числе рантайм-компонент и интерпретаторов/ВМ**);
- динамический анализ – модульное и функциональное тестирование (подтверждение известного);
- динамический анализ – фаззинг-тестирование (поиск неизвестного);
- динамический анализ – выявление побочных взаимодействий со средой функционирования;
- динамический анализ – анализ утечек чувствительных (помеченных) данных;
- тестирование на проникновение.

Автоматизация практик безопасной разработки (встраивание в CI/CD).
Обучение студентов и сотрудников в парадигме безопасной разработки.

2.3. Сертификация. Перспективы

- автоматизация и стандартизация определения ширины и глубины поверхности атаки в процессе безопасной разработки продуктов и их сертификации;

- стандартизация использования системных компонент (ядра, системное ПО, компоненты виртуализации и контейнеризации, компоненты сборочной системы);

- стандартизация использования сторонних компонент с открытым исходным кодом (ядра, системное ПО, компоненты виртуализации и контейнеризации, компоненты сборочной системы);

- разработка и обновление ГОСТов по Безопасной разработке, Статическому и Динамическому анализу, Безопасной компиляции и т.д., а также Требований отечественных Регуляторов;

и многое, многое другое!

2.4. Сертификация. Технологии безопасности ИСП РАН

«На поршневом самолёте нельзя улететь на луну.
Даже если «сейлы» утверждают обратное» ©

- статический ММКЧ-анализ с динамическим учетом параметров компиляции/компоновки и использованием доказательных возможностей SMT-решателей для ЯП: C/C++, C#, Java, Go (**SVACE** – основной стат. анализатор в Samsung, Huawei, Лаборатория Касперского и мн. др.);

- динамический фаззинг-анализ: низкоуровневого кода, с использованием технологий символьного выполнения и предикатов безопасности, с возможностями сбора покрытия по базовым блокам низкоуровневого кода, с возможностями оркестрации и мн. др. (**CRUSHER**);

- широчайший спектр технологий полносистемной интроспекции, в том числе для анализа распространения помеченных данных и определения поверхности атаки (**БЛЕСНА …**);

- анализ и создание компонентов сборочной системы (**БЕЗОПАСНЫЙ КОМПИЛЯТОР**);

- и многое, многое другое: https://www.ispras.ru/technologies.

2.5. Сертификация. Центры компетенций

- технологический центр исследования безопасности ядра Linux (совместно со ФСТЭК России), ведущий работы по исследованию, повышению защищенности и стандартизации Linux-ядер;

- центр доверенного искусственного интеллекта (при поддержке правительства России), ведущий работы по выявлению и противодействие угрозам, специфичным для технологий ИИ; повышению интерпретируемости моделей машинного обучения; создание ПО и облачной платформы для разработки доверенных систем, использующих ИИ;

- технологический центр исследования безопасности наиболее значимых пакетов с открытым исходным кодом (совместно со ФСТЭК России). Запланированы работы по исследованию, повышению защищенности и стандартизации общеупотребимой пакетной базы.

Все вышеуказанные работы планируется проводить с привлечением широкого круга экспертов сообщества, студентов и аспирантов

2.6. Сертификация. Сообщество и методическая база

Информационные и методические ресурсы:

- телеграм-каналы под эгидой Центра компетенций ФСТЭК России и ИСП РАН
- видеолекции ФСТЭК России и ИСП РАН по динамическому и статическому анализу
- методические материалы по статическому и динамическому анализу
- документы сообщества Центра компетенций
- репозитории «анализатор as a service» для статического и фаззинг-анализа

Благодарим коллег из ГРОТЕК за предоставленную возможность выступить на мероприятии:

- запись конференции «Актуальные вопросы защиты информации» в рамках «ТБФорум 2022» от 16 февраля: https://www.youtube.com/watch?v=Zz9zOj9Z6SE

- предыдущая версия данной презентации с ссылками на различные материалы: https://www.tbforum.ru/2022/program/information-security

3.1. Наш опыт. Внедрение безопасной разработки - тезисы

1. SDL – это в первую очередь про людей, и только потом про инструменты.

2. Мультифункциональные комбайны класса «серебряная пуля» не помогут вам в борьбе с серьезными нарушителями.

3. Нормативно-правовая база отечественных Регуляторов (в частности ФСТЭК России) задаёт высокую планку требований, и в ряде пунктов опережает мировые стандарты. Особенно с учетом нововведений в кратко- и среднесрочной перспективе.

4. Важнейшим аспектом успешного внедрения SDL на уровне компании в целом является понимание собственниками компании необходимости и неотвратимости данной парадигмы.

5. Важнейшим аспектом успешного внедрения SDL на уровне компании в целом является борьба с рутиной.

6. В отличие от «ИБ на аутсорс» (в частности SOC) качественного «SDL на аутсорс» **не существует!**

3.2. Наш опыт. Внедрение безопасной разработки - стратегия

- поставить цель и **проявить политическую волю**;

- сформировать команду профессионалов:
  - на внедрение SDL-практик в компании с командой 5-15 разработчиков необходимо 1-2 выделенных SDL-специалиста: Junior/Middle-разработчик по каждому ЯП, используемом в продукте, навыки пентеста и общее представление об анализе уязвимостей, devops-навыки, «горящие глаза» и «прямые руки»;
  - хороший SDL практически не реализуем без хорошего **DevOps-специалиста**;
  - свободных Security Champion на рынке **нет**. Но такого специалиста реально **вырастить**;

- запустить процесс и подождать 6-12 месяцев (срок на базовое освоение и внедрение SDL-практик при правильной мотивации команды).

Освоение полезного и сложного инструментария нужно начинать вчера!

3.3. Наш опыт. Внедрение безопасной разработки - тактика

1. Инвентаризация. Убрать лишний код (в частности избыточные интерпретаторы), уменьшив поверхность атаки (ПА)

2. Начинать писать ЗБ/ТУ правильно и сразу прикидывать под это тесты (Test Second если Test First не тянем)

2. Фиксация и оформление схемы ПА

3. Разработка схем технического и эскизного проекта

1. Выстраивание Devops-процесса:

- автоматический контроль CVE
- сборка всего из локальных репозиториев полностью из исходников (можно в несколько итераций)

2. Внедрение SVACE

2. Для как минимум все модулей ПА запуск всех мод. и регр. тестов в комплекте 3rd party при RC-сборках

3. Создание концепции дин. анализа на основе CRUSHER и открытых решений для managed-кода

- механизмы фаззинга
- сбор покрытия

1. Люди (искать правильных людей):

-фаззингист (старший и джун-помощник для наращивания числа фаззинг-целей – или как в Касперском, разработать тулчейн и стандарт и отдать в команды задачу формирования первичных целей)

- тех. писатель
- devops (хороший девопс очень важен)
- стат. анализ (все инженеры понемногу, или также выделенный специалист)).

2. Подключение к ресурсам и репозиториям сообщества Центра компетенций

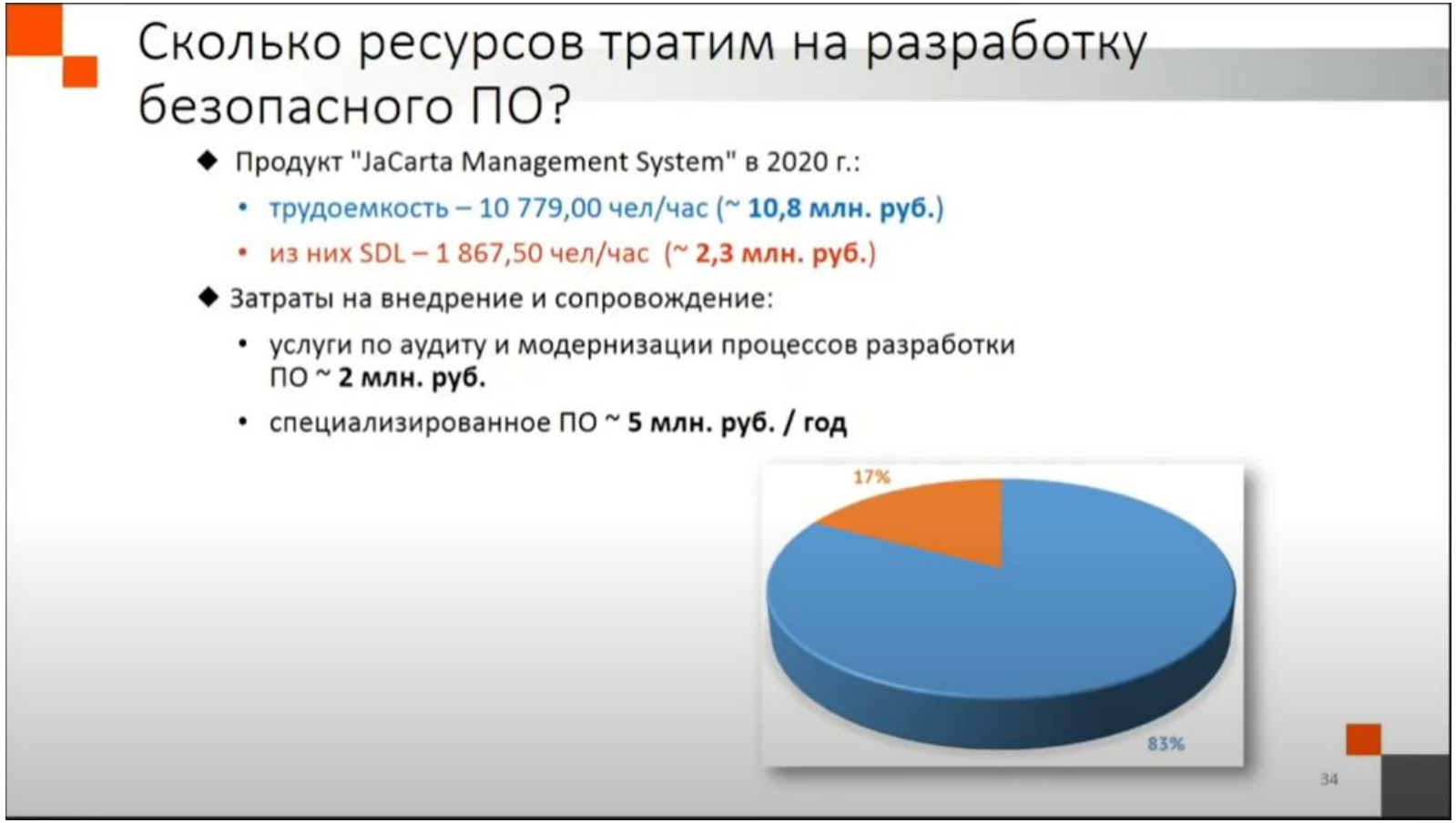
3.4. Наш опыт. Внедрение безопасной разработки - ресурсы

Технические затраты

- создать инфраструктуру: аппаратная платформа-вычислитель (1 млн. – 6 млн.), в том числе возможна аренда в облаке;

- развернуть необходимые инструментальные средства (до 5 млн. в год);

Опыт наших друзей из Аладдин Р.Д



Тезисы вебинара «Разработка безопасного ПО для предприятий КИИ, АСУ ТП, гос. структур» доступного по адресу https://www.youtube.com/watch?v=2TCscvm66aA

Благодарю за внимание!

Дмитрий Пономарев
ООО НТЦ «Фобос-НТ» / ИСП РАН
(@DmitryJustDmitry)