Системный подход при разработке и сертификации безопасного и качественного ПО

Дмитрий Пономарев

технический директор **ООО НТЦ «Фобос-НТ»**
сотрудник **ИСП РАН**

ТГ: @DmitryJustDmitry

Системный подход к решению вопросов IT-безопасности государства

Напряженная политическая обстановка. **Президентом РФ** поставлена задача достижения **Технологической независимости** (импортозамещение – первый шаг). Критически важны:

- суверенизация критических разработок
- разработка систем в парадигме доверенности как базового принципа
- создание «позиций» в мировом OpenSource

Традиционный подход к защите информации:

- физическая, административная защита и формирование политик организации
- привлечение SOC для выявления нестандартных и APT угроз
- наложенные средства (NGFW, антивирусы, сканеры уязвимостей и т. п.)

Недостаточно!

Системный подход к решению требует гораздо большего:

- проектирование и разработка приложений в парадигме безопасной разработки
- формирование «школы» продуктовой безопасности, инженерной и образовательной культуры
- создание государственных центров компетенций по углубленному анализу критических компонентов

Некоторые технологии и принципы безопасной разработки

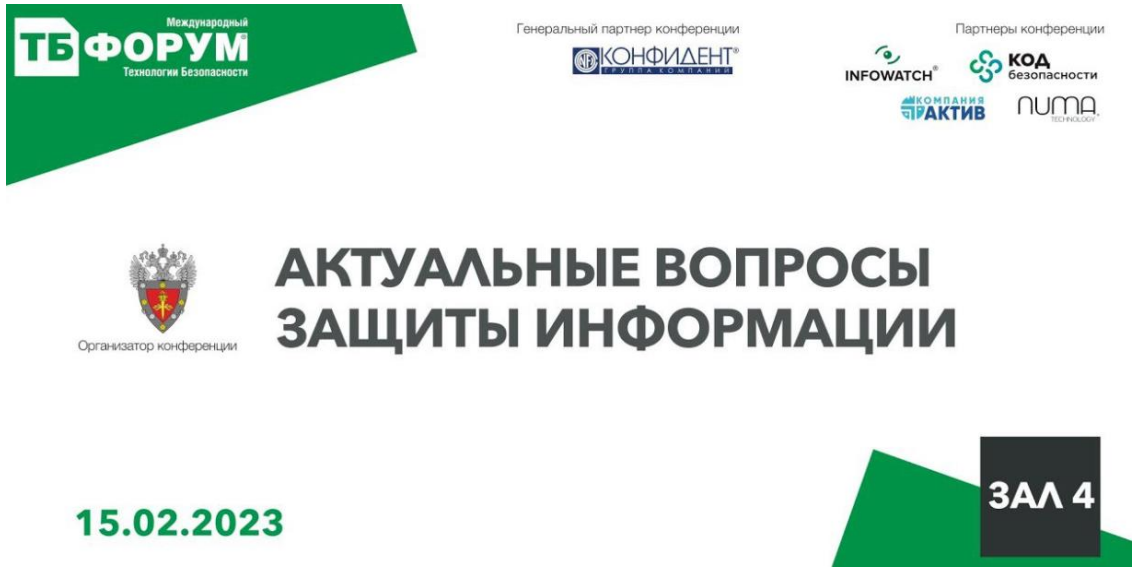
- **обучение студентов-стажеров и сотрудников в парадигме безопасной разработки**

- моделирование и проектирование безопасной архитектуры
- анализ безызбыточности внешних интерфейсов и прав доступа к ресурсам
- статический анализ исходного кода
- статический анализ конфигураций модулей и контейнеров
- использование безопасных тулчейнов (*компоновщики и их параметры*)
- выявление и устранение рисков от известных уязвимостей сторонних компонентов
- модульное и функциональное тестирование (подтверждение известного
- фаззинг тестирование (*поиск неизвестного*)
- выявление недекларированных взаимодействий со средой функционирования
- анализ утечек чувствительных данных
- классическое тестирование на проникновение (*в первую очередь в отношении сетевых сервисов*)

- **автоматизация и борьба с рутиной (встраивание SDL практик в CI/CD)**

А не решающая все проблемы волшебная флешка-анализатор за много Х денег…

ТБ Форум 2023. Широкий спектр вопросов ИБ в фокусе внимания ФСТЭК России



15е февраля – организатор ФСТЭК России

Актуальные вопросы защиты информации. XIII конференция

16е февраля - встреча SDL-сообщества

Безопасная разработка. Подходы и инструменты управления процессом

Основные проблемы:

- нас слишком мало для масштаба вызовов времени
- традиционно нехватка «горизонтального» и «вертикального» доверия
- более 50% времени тратим на одно и то же

Основные цели:

- обмен опытом и лучшими практиками между энтузиастами одного дело
- укрепление доверия между государственными и частными организациями
- объединение усилий в зонах неконкурентности
- формирование благоприятных условий для развития образования, в первую очередь в регионах

Центры компетенций ФСТЭК России и ИСП РАН

Федеральная служба по техническому и экспортному контролю

ИСП РАН

ИНСТИТУТ СИСТЕМНОГО ПРОГРАММИРОВАНИЯ ИМ. В.П. ИВАННИКОВА РОССИЙСКОЙ АКАДЕМИИ НАУК

Сборник технологий ИСП РАН за 2022 год

Коммуникационные ресурсы сообщества энтузиастов под эгидой Центра компетенций (телеграм-чаты)

Технологические центры исследования безопасности ядра Линукс и критических компонентов

Технологический центр исследования безопасности ядра Linux

- создан ФСТЭК России на базе ИСП РАН
- 22 партнёра:
  - АО «Аладдин Р.Д.»
  - ООО «Айдеко»
  - ООО «Базальт СПО»
  - АО «Байкал электроникс»
  - ООО «БЕЛЛСОФТ»
  - АО «ИВК»
  - АО «ИнфоТеКС»
  - ООО «ИТБ»
  - ООО «Код Безопасности»
  - ООО «Конфидент»
  - АО НТЦ «Модуль»
  - АО «МЦСТ»
  - АО «НППКТ»
  - ООО «Открытая мобильная платформа»
  - АО «РАСУ»
  - ООО «РЕД СОФТ»
  - ООО «РусБИТех-Астра»
  - АО МВП «Свемел»
  - ООО «НТЦ ИТ РОСА»
  - ООО «Фактор-ТС»
  - АО «ФИНТЕХ»
  - ООО «ЯНДЕКС.ОБЛАКО»

Подготовка исправлений

Компания	Количество принятых патчей
ООО «Базальт СПО»	1
ООО «БЕЛЛСОФТ»	7
АО «ИнфоТеКС»	3
ИСП РАН	44
ООО «Открытая мобильная платформа»	24
АО «РАСУ»	3
ООО «РЕД СОФТ»	3
ООО «РусБИТех-Астра»	6
АО МВП «Свемел»	1
ООО «Фактор-ТС»	4
ООО «ФИНТЕХ»	4
ООО «ЯНДЕКС.ОБЛАКО»	5
Всего:	**105**

Технологический центр исследования безопасности ядра Линукс

Развитие системы образования и формирование содружества ВУЗов

Проблемы:

- системный кадровый голод. «Фронтендеры» есть, «системщиков» не хватает
- устаревшие, поверхностные или коммерчески-ориентированные методики

Подходы к решению проблем:

- физтеховский «треугольник»: образование, инновации, производство
- создание новых специальностей (в России **не учат** на AppSec`а)
- ***академик Аветисян А.И.*: «Качественное образование в данной сфере практически невозможно без хороших «семинаристов»»**

Новая специальность «Кибербезопасность», первый набор в магистратуру ВШЭ в 2022 г.

Энтузиасты из Новгород(ов), Орла, Чебоксар, Еревана, Москвы и других городов развивают и популяризуют методики обучения – растят будущую «**гвардию**» отрасли безопасности, в том для нужд собственных организаций! Участие сейчас обеспечит вашей организации долгосрочную перспективу.

Дискуссия по вопросам образования в чате сообщества «Орг. вопросы» ->

ИСП РАН – образовательный центр и место притяжения единомышленников

OS DAY
Крупнейшая конференция по вопросам Open Source

Иванниковские чтения
Выездная молодежная конференция

ISPRASOPEN
Главная ежегодная отчетная конференция в здании Президиума РАН

Лекции по безопасной разработке на ресурсе ***БДУ ФСТЭК России***

Лекции ***Падаряна В. А.*** *по основам системного программирования и информационной безопасности*

Взгляд в будущее – от идей и прототипов к промышленным стандартам

Создание **унифицированного комплекса**, «под ключ» решающего задачи ->

- интеграции средств разработки, анализа, хранения кода

- достижения кумулятивного эффекта от связной работы средств анализа ИСП РАН (**Svace, Crusher, Sydr, Natch** и т. д.) и единого портала аналитики

- предоставления модульной инфраструктуры, позволяющей выполнять сравнительное тестирование инструментов анализа и интеграцию их в базовую поставку, *например*:
  - средства анализа исходного кода на закладки и уязвимости **Ростелеком Solar**
  - инструменты компонентного анализа и проверки лицензионной чистоты **CodeScoring**

- поддержки локальных и облачных развертываний комплекса с возможностью миграции задач между рабочими станциями и **Центрами компетенций**

- интеграции с наработками **Центра доверенного искусственного интеллекта**, созданного на базе ИСП РАН по заданию Правительства РФ ->

А теперь - про деньги
Мы же на бизнес-форуме ☺

Марк Коренберг, технический лидер и ген. директор ideco (разработчик **Ideco UTM**)

«*Разговаривая с **генеральным** директором компании держи в голове, что, как правило, по настоящему его волнуют только два вопроса:*

*- как то, что ты предлагаешь, может помочь компании **терять (и тратить) меньше***

*- как то, что ты предлагаешь, может помочь компании **заработать больше**»*

Безопасная разработка - домен качественной разработки

Дмитрий Шмойлов, Лаборатория Касперского

«*Повсеместное внедрение и автоматизация процедур тестирования и безопасной разработки позволило сократить релизный цикл основных продуктов компании с 6 месяцев до 2 недель*»

Антон Бауткин, Аладдин Р Д

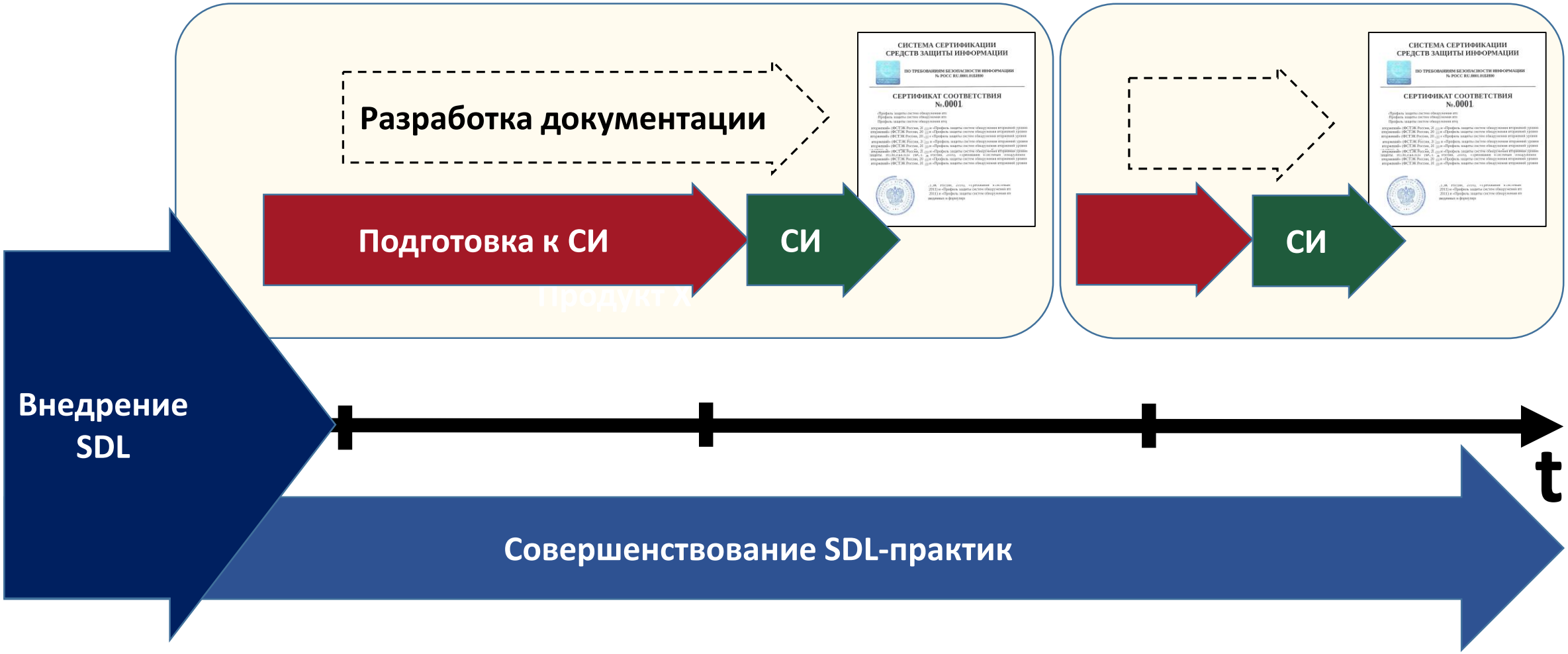
«*Внедрение и развитие на постоянной основе комплекса практик анализа и тестирования продуктов привело к системному уменьшению числа ошибок, выявляемых на этапе эксплуатации*»

Переход к парадигме безопасной и качественной разработки:

- **потребует** ресурсов в краткосрочной перспективе;
- **принесёт** ещё больше в долгосрочной за счет **снижения:**
  - Time To Market
  - числа рекламаций

Конечно же, если вы не фирма-однодневка…

Сертификация «по ФСТЭК» в парадигме SDL-First (подход лаборатории Фобос-НТ)



Что это значит для бизнеса:

- **предсказуемые сроки** получения сертификата соответствия
- в первую очередь **вклад в свою команду**, а не в лабораторию за «*магические действия*»

Несколько слов про нашу лабораторию

В течение последних 5 лет проводим ежегодный аудит SDL-процессов в АО «Лаборатория Касперского»

Организовывали и участвовали совместно с ИСП РАН, ООО «Код Безопасности» и АО «Лаборатория Касперского» в 2019 году в апробации первой редакции Методики ВУ и НДВ ФСТЭК России

Участвуем в подготовке и проведении образовательных курсов ФАУ "ГНИИИ ПТЗИ ФСТЭК России“ на базе ИСП РАН: программы №31 «Фаззинг-тестирование» и №33 «Архитектурный анализ», принимаем активное участие в разработке проектов Требований к Средствам Виртуализации, Средствам Контейнеризации, СУБД, а также Методики ВУ и НДВ

Оказываем методическую и практическую помощь в становлении и улучшении SDL-процессов и процессов 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», ЗАО «Институт Сетевых Технологий», ООО «Код Безопасности», ООО «НПЦ КСБ»,
АО «Лаборатория Касперского», ООО «Постгрес Профессиональный», ООО «R-Vision»,
ООО «Нума Технологии», ООО «Secret Technologies», ООО «Cyberpeak» и многим другим…

Рубрика «добрый пиар». Гарда Технологии - SDL-энтузиасты из Ниж. Новгорода

БЕЗОПАСНАЯ РАЗРАБОТКА

ГАРДА ТЕХНОЛОГИИ

ВНУТРИ КОМПАНИИ

СТАТИЧЕСКИЙ АНАЛИЗ

- **> 50 ПРОЕКТОВ** — Прошло через статический анализ
- **> 500 СНИМКОВ** — Проанализировано
- **571 ОШИБКА** — Исправлена по результатам работы статического анализатора

ДИНАМИЧЕСКИЙ АНАЛИЗ

- **~200 ТОЧЕК ВХОДА** — Для различных продуктов
- **15 МОДУЛЕЙ** — Как собственных проектов, так и сторонних приложений, включая nginx и libreoffice.
- **14 ОШИБОК** — Исправлено по результатам анализа

КАК УЧАСТНИК СООБЩЕСТВА ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ (НА РЕСУРСАХ ИСПРАН)

- **4 ПРОЕКТА** — NET Core, nginx, suricata, RE2
- **> 400 МАРКЕРОВ** — NET Core, nginx, suricata
- **> 140** — Человеко-часов
- **13 ЗАПРОСОВ** — Natch

Отличный пример того, что «дорогу осилит идущий»!

Что ещё посмотреть и почитать

Безопасность в тапочках - подкаст с Нижегородскими корнями

ИСП РАН

Как правильно организовать процесс безопасной разработки ПО (SDL): 6 шагов

30/12/22 11 min read

ФСТЭК

Безопасная разработка и сертификация: две стороны одной медали

Статьи в журнале Информационная безопасность

Сайт испытательной лаборатории (ФСТЭК, ФСБ, МО) и органа по аттестации ООО НТЦ Фобос-НТ

Благодарю за внимание!

Дмитрий Пономарев

технический директор **ООО НТЦ «Фобос-НТ»**
сотрудник **ИСП РАН**

ТГ: @DmitryJustDmitry