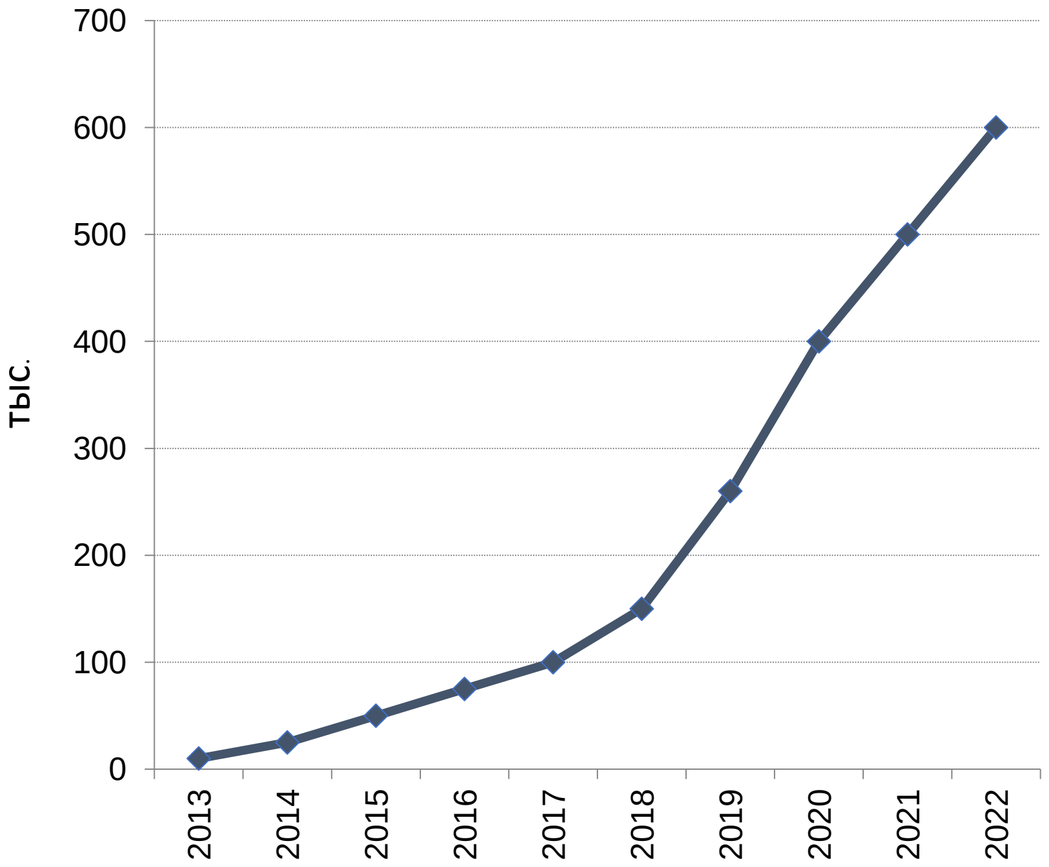
Процессы и инструменты разработки безопасных ОС

Специалист по тестированию и анализу уязвимостей ПО, к.т.н.,
Туманов Юрий

rosalinux.ru

2022

Угрозы ИБ



Динамика количества киберпреступлений
(по данным Генпрокуратуры РФ)

Проблемы образования в сфере ИБ

Проблемы учащихся:

- неясные перспективы;
- невысокая популярность у абитуриентов;
- высокий проходной балу;
- низкая «выживаемость» - 50% отчислят.

Проблемы преподавательского состава:

- крайняя забюрократизированность;
- зарплата – ну такое;
- молодые специалисты не идут;
- мало преподавателей.

Атаки на цепочки поставок и вопрос доверия вендору

Атака на цепочки поставок – на одном из этапов жизненного цикла ПО в него или в один из компонентов, обеспечивающих его работу, был внедрён вредоносный код, функциональность которого будет реализована у конечного пользователя ПО.

Атака может быть реализована одним из следующих вариантов:
- успешная атака либо на средство сборки ПО, либо на инфраструктуру обновлений;
- атака на доверенных пользователей, обладающих доверенными сертификатами;
- вредоносный код внедряется в стороннее ПО, которое использует ПО, которое поставляет вендор ;
- заранее внедрённый вредоносный код в аппаратные средства.

Каковы необходимые и достаточные требования к безопасности ПО?

Лирика и эмпирика:

• уровень критичности уязвимости (cve) пакетов, полученный из баз данных уязвимостей – с какого точно надо закрывать?

• уровень критичности дефектов (cwe) в коде пакетов, полученный в результате статического анализа – что важно?

• по динамике (фаззингу) – глубина покрытия, алгоритмы – что важно?

• антивирусный анализ – нет, ну правда?

• требования по пентесту – наборы тестов?

Источники угроз в организации

Внутренний нарушитель

Внешний нарушитель

ОС РОСА «КОБАЛЬТ» ФСТЭК

- Сертифицирована в Системе сертификации средств защиты информации по требованиям безопасности информации
- Сертификат соответствия № 4039 (выдан ФСТЭК России, срок 07.12.2023 г.).
- Соответствует требованиям методического документа ФСТЭК «Профиль защиты операционных систем типа «А» четвертого класса защиты ИТ.ОС.А4.ПЗ» и требованиям по безопасности информации согласно приказу ФСТЭК № 76 по четвертому уровню доверия.
- Предназначена для использования:

  - в государственных информационных системах 1 класса защищенности в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утв. приказом ФСТЭК России от 11.02.2013 г. № 17;
  - в информационных системах персональных данных 1 уровня защищенности в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. приказом ФСТЭК России от 18.02.2013 г. № 21.

Сертифицированная версия ROSA VIRTUALIZATION

- Проходит сертификацию на соответствие «Требованиям по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утв. приказом ФСТЭК России от 2 июня 2020 года № 76) - по 4 уровню доверия (решение ФСТЭК России № 6786 от 7 февраля 2022 г.).
- Предназначена для использования **(после сертификации):**

  - в государственных информационных системах 1 класса защищенности в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утв. приказом ФСТЭК России от 11.02.2013 г. № 17;
  - в информационных системах персональных данных 1 уровня защищенности в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. приказом ФСТЭК России от 18.02.2013 г. № 21.

Механизмы защиты от нарушителя в ОС РОСА Linux

- Идентификация, аутентификация и авторизация пользователей ОС
- Управление доступом
- Обеспечение доступности ресурсов
- Обеспечение целостности, восстановления и резервного копирования компонентов ОС
- Защита от несанкционированного доступа в обход правил управления доступом
- Фильтрация сетевого потока
- Регистрация событий безопасности ОС
- И другие…

What the ABF?!

ABF (Automatic Build Farm) – это распределенная среда разработки и сборки программных продуктов для ОС РОСА Linux и создания дистрибутивов на их основе

- over > 50000 опенсорс-пакетов в репозитории;
- git-совместимый интерфейс;
- сборка под различные аппаратные платформы;
- интерфейсы, знакомые как разработчикам, так и мэйнтейнерам;
- российский программно-аппаратный комплекс, физически находящийся на территории РФ.

Работа со студентами

- Курс «Безопасная разработка программного обеспечения» для студентов НИЯУ «МИФИ», обучающихся на кафедре №42 «Криптология и кибербезопасность»

- Мастер-класс по использованию статического анализатора Svace

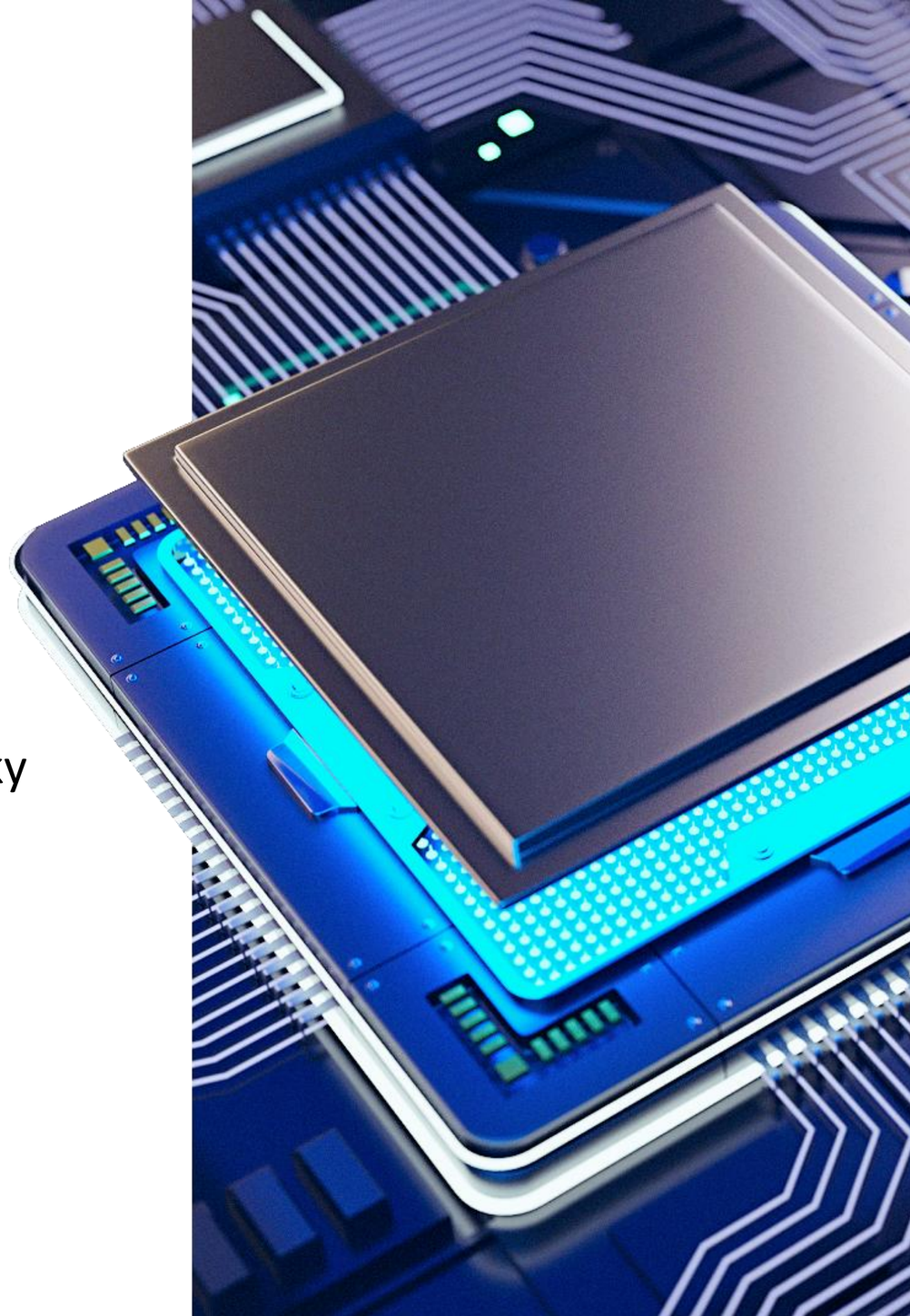
- Планы на дальнейшее взаимодействие

Безопасная разработка в НТЦ ИТ РОСА

1. Анализ требований
2. Архитектура и дизайн
3. Разработка
4. Тестирование
5. Выпуск и поддержка
6. Вывод из эксплуатации

Использованные решения:

- **уровень критичности уязвимости(cve)** – внутренняя разработка – package scanner
- **уровень критичности дефектов (cwe)** – статический анализатор Svace
- **фаззинг** – afl++
- **антивирусный анализ** – Kaspersky AV, Dr.Web
- **пентесты** – различные пакеты, входящие в поставку Kali Linux (nmap, metasploit framework, OpenVas, Burp Suite, …)



Процессы и инструменты разработки безопасных ОС

- Регулярно отслеживать информацию по открытым источникам о новых уязвимостях и проводить чекап на их наличие

- Развивать инфраструктуру доверенных вендоров ПО, безопасных репозиториев

- Ценить труд людей и платить достойные зарплаты в основополагающих профессиях, в том числе преподавателям

- Следить за трендами в сфере реальной информационной безопасности, интегрировать их в стандарты

Спасибо за внимание!

sales@rosalinux.ru

rosalinux.ru

+7 (495) 137-88-44