

# Инструмент анализа бинарного кода Aegis

Шамиль Курмангалеев [kursh@ispras.ru](mailto:kursh@ispras.ru)

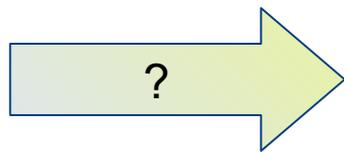
Григорий Иванов [gregory@ispras.ru](mailto:gregory@ispras.ru)

## ТЕМЫ:

- ✓ Мотивирующий пример
- ✓ Методы поиска ошибок
- ✓ Автоматизация анализа
- ✓ Задачи
- ✓ Темы для курсовых
- ✓ С чем будете работать

- CVE-2021-34401: **NVIDIA Linux kernel** distributions contains CodeExec
- CVE-2021-44733: **Linux kernel** through 5.15.11 contains CodeExec
- CVE-2021-40029: **Samba** contains CodeExec
- CVE-2021-43217: Windows **Encrypting File System** (EFS) contains Remote CodeExec
- CVE-2021-3682: **qemu** contains CodeExec on host

- По исходному коду
- По бинарному



## Полноценное исследование

```
1 /*
2  * Copyright 2013-2021 The OpenSSL Project Authors. All Rights Reserved.
3  *
4  * Licensed under the Apache License 2.0 (the "License"). You may not use
5  * this file except in compliance with the License. You can obtain a copy
6  * in the file LICENSE in the source distribution or at
7  * https://www.openssl.org/source/license.html
8  */
9
10
11 /* Simple AES CCM authenticated encryption with additional data (AAD)
12  * demonstration program.
13  */
14
15 #include <stdio.h>
16 #include openssl/err.h
17 #include openssl/bio.h
18 #include openssl/evp.h
19 #include openssl/core_names.h
20
21 /* AES-CCM test data obtained from NIST public test vectors */
22
23 /* AES key */
24 static const unsigned char ccm_key[] = {
25     0xc0, 0xb0, 0xb9, 0xae, 0xd4, 0x45, 0x51, 0xf6, 0xad, 0xf0, 0xe6,
26     0xb3, 0x6f, 0x45, 0x55, 0x5d, 0xd0, 0x47, 0x23, 0xba, 0xad, 0x48, 0xc8
27 };
28
29 /* Unique nonce to be used for this message */
30 static const unsigned char ccm_nonce[] = {
31     0x76, 0x40, 0x43, 0xc4, 0x94, 0x60, 0xb7
32 };
33
34 /*
35  * Example of Additional Authenticated Data (AAD), i.e. unencrypted data
36  * which can be authenticated using the generated Tag value.
37  */
38 static const unsigned char ccm_adata[] = {
39     0x6e, 0x00, 0xd1, 0x77, 0x1b, 0xad, 0xf3, 0xa1, 0xc9, 0xab, 0x25, 0xc7,
```

**GIT:** История коммитов, патчи на уже известные CVE, открытые ISSUE

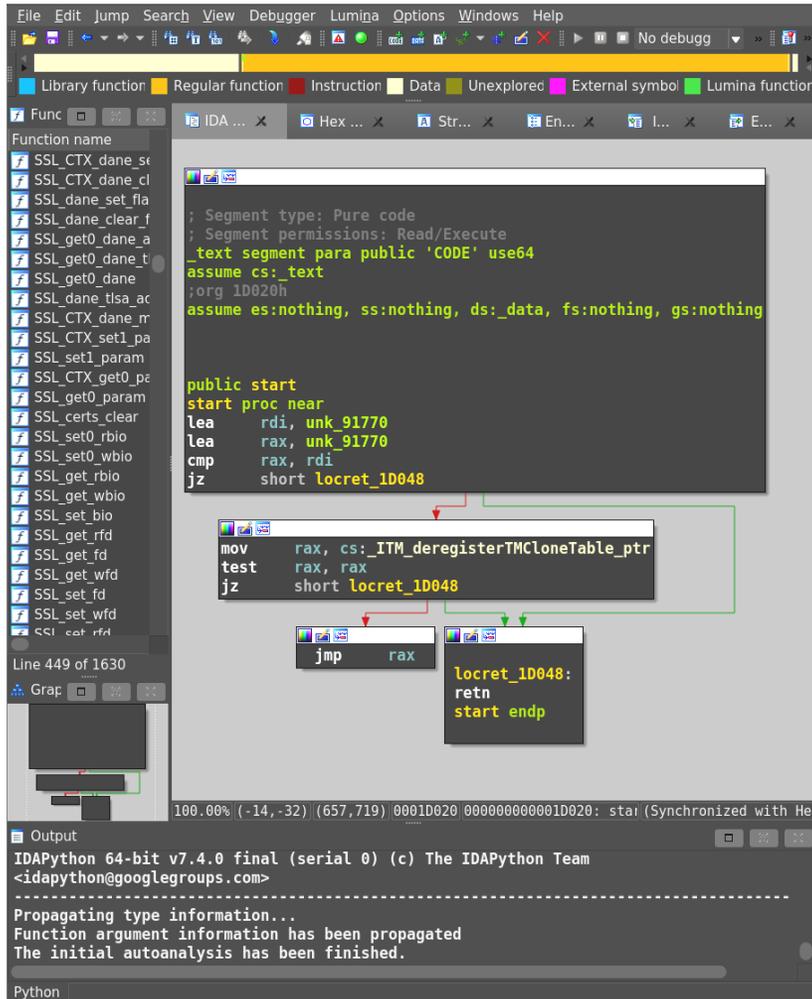
**ИСХОДНЫЙ КОД:** комментарии, TODO/FIXME, стат. анализ IDE (восстановление потока данных и управления, графы вызовов, UML-диаграммы), scitools Understand

**ИСПОЛНЯЕМЫЕ МОДУЛИ:** наличие ASLR, права доступа на секции, секции импорта и экспорта, строки, отладочная информация

**ИСПОЛНЯЕМЫЙ КОД:** дизассемблер (IDA Pro, Ghidra, r2\*, Binary Ninja\*), декомпилятор (HexRays, Ghidra-decompiler), анализаторы (Angr, \*Miasm)

\* не является промышленным инструментом или не удовлетворяет требованиям

# ✓ МЕТОДЫ ПОИСКА ОШИБОК (продолжение)



**СБОРКА:** Сообщения компилятора (родные и указанные дополнительно), команды линковки, флаги компиляции (+ стат. анализатор gcc)

**СТАТИЧЕСКИЕ АНАЛИЗАТОРЫ:** Clang, gcc static analyzer, SonarQube, CodeQL (открытые). Svsace\*\*, Perforce2, Coverity (Закрытые)

**ОТЛАДЧИКИ:** gdb, WinDbg, OllyDbg, qemu

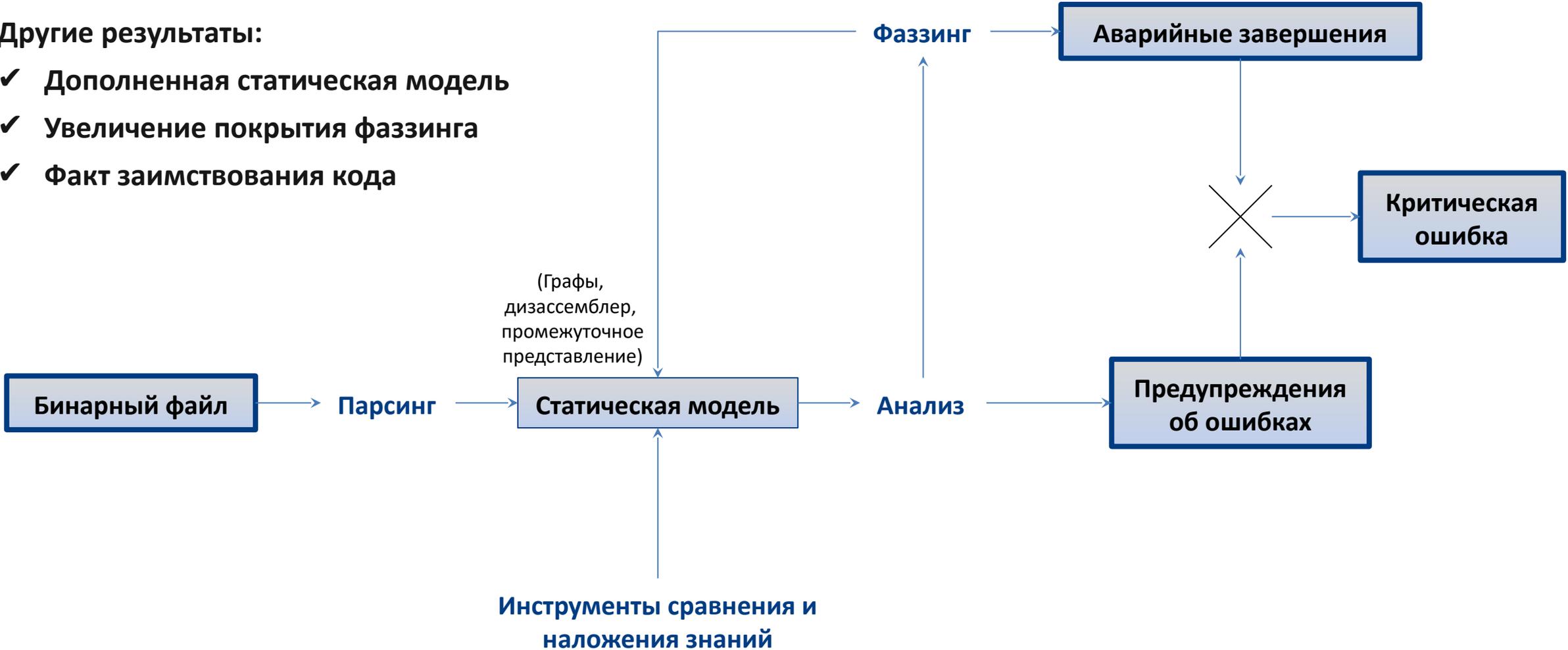
**ФАЗЗЕРЫ:** Afl (+форки), libfuzzer, Syzkaller, honggfuzz, nух, jacklope, Crusher\*\*

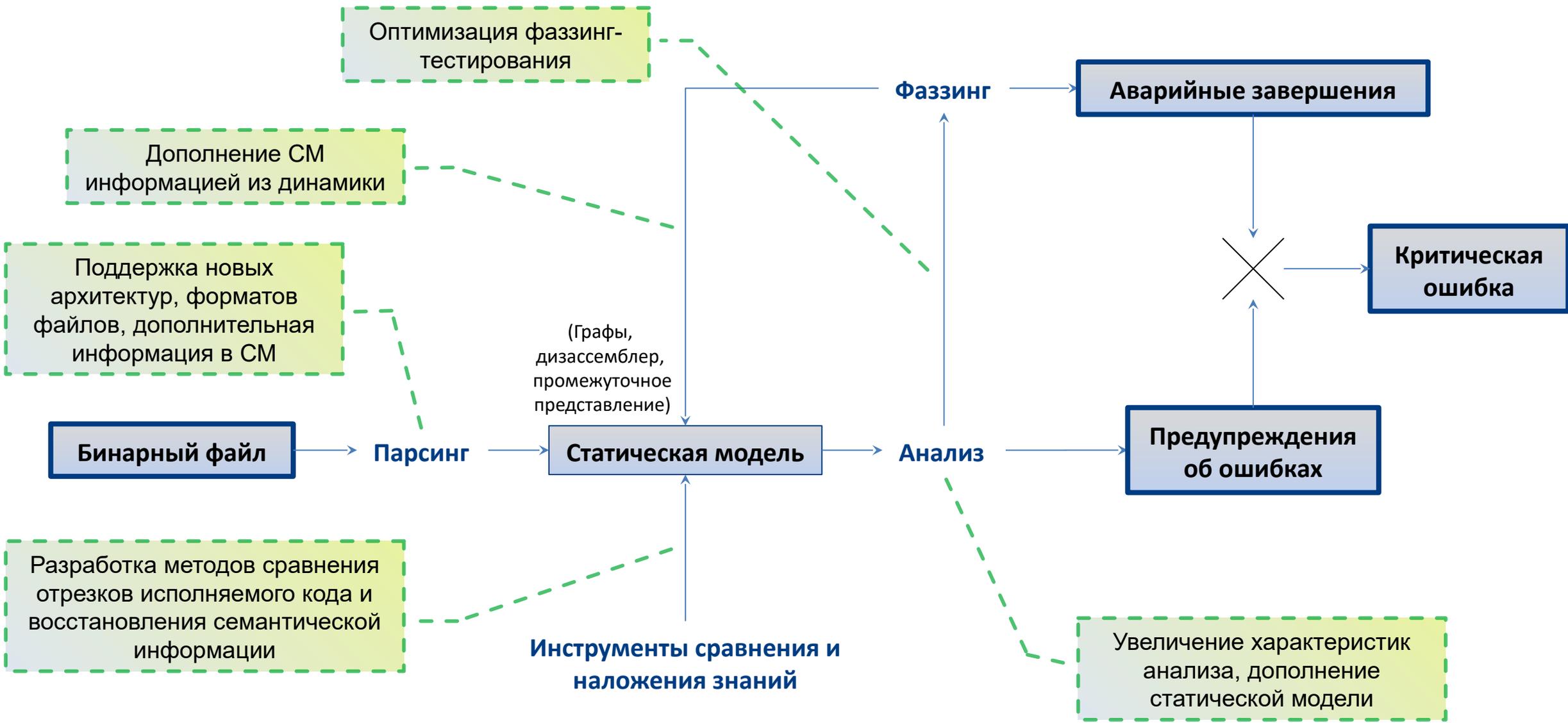
**ДИНАМИЧЕСКИЕ АНАЛИЗАТОРЫ:** strace, DrMemory, Valgrind, afl-analyze

\*\* Разработан и успешно используется в ИСП РАН

**Другие результаты:**

- ✓ Дополненная статическая модель
- ✓ Увеличение покрытия фаззинга
- ✓ Факт заимствования кода



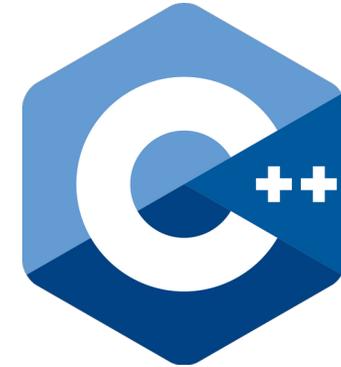
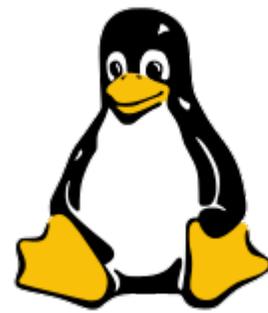


## ТЕМЫ:

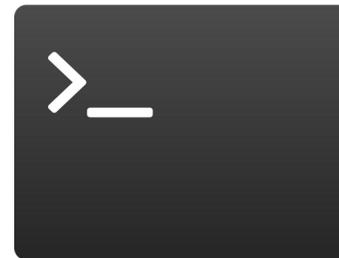
- ✓ Оптимизация промежуточного представления для облегчения статического анализа
- ✓ Разработка детекторов ошибок для анализа бинарного кода
- ✓ Уточнение статической модели информацией из динамического анализа
- ✓ Автоматизированная генерация трансляторов промежуточного представления REIL
- ✓ Разработка методов восстановления карты динамической памяти

**Инициативные темы приветствуются!**

- ✓ Си/C++
- ✓ Ассемблер
- ✓ Операционные системы
- ✓ Компиляторы
- ✓ Linux-окружение
- ✓ Скриптовые языки: Bash, Python
- ✓ Фаззеры
- ✓ Статические анализаторы
- ✓ Символьные решатели



# BASH



ИСП РАН

# Спасибо!

## Приходите!

Курмангалеев Шамиль - [kursh@ispras.ru](mailto:kursh@ispras.ru)

Иванов Григорий - [gregory@ispras.ru](mailto:gregory@ispras.ru)