Испытательная лаборатория
ООО Научно-технический центр «Фобос-НТ»

Радости и горести современной сертификации

Борзов Роман
Кузнецов Андрей

Испытательная лаборатория ООО НТЦ «Фобос-НТ»

1. Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00.
Аттестат аккредитации испытательной лаборатории СЗИ RU.0001.01БИ00.Б039, выдан ФСТЭК России 20 марта 2020 г.

2. Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (Система сертификации СЗИ-ГТ) РОСС RU.0003.01БИ00.
Аттестат аккредитации СЗИ RU.ЛИ0162, выдан ФСБ России 22 декабря 2020 г.

3. Система сертификации средств защиты информации по требованиям безопасности информации Министерства обороны Российской Федерации.
Аттестат аккредитации испытательной лаборатории № 401 от 06 июня 2022 г.

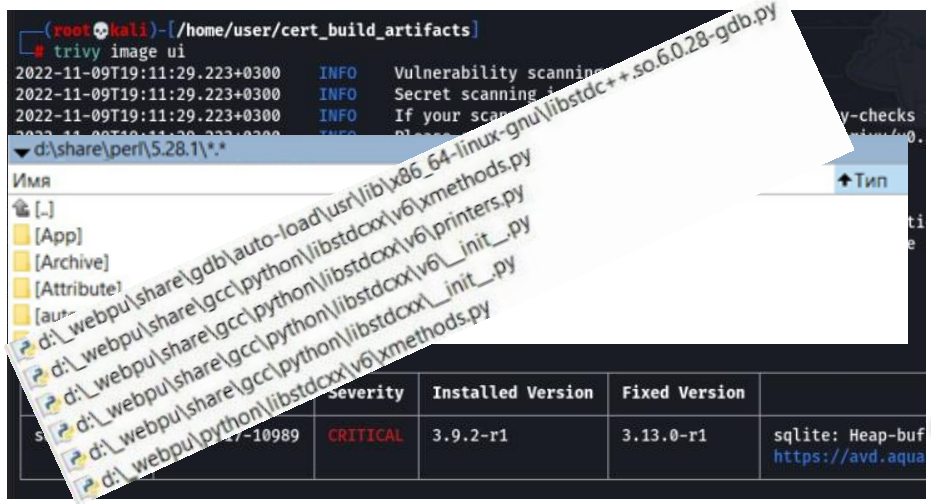
Горести

Управленческие

- Смотрите, у нас уже всё есть, когда будет сертификат?
- Продукт уже есть, давайте быстро сделаем документы!
- Нам нужен сертификат! Ресурсов очень мало, это не основное направление…
- Сделаем все на этой неделе, до пятницы точно скинем!
- Зачем собирать из исходников, что за требование? *Нормально же сидели…*

Инженерные

- У нас всё в контейнерах, это безопасно!
- Эти CVE не эксплуатируемы.
- Какие ещё интерпретаторы?!
- Что ещё за поверхность атаки?!
- Эти модули ни на что не влияют!



У нас всё в контейнерах, это безопасно!


```
{
  "id": "robotattack",
  "title": "Return Of Bleichenbacher's Oracle Threat",
  "desc": "ROBOT is the return of a 19-year-old vulnerability that allows perf
  "descriptions": [
    {
```


```
└─# trivy image ui
2022-11-09T19:11:29.223+0300    INFO    Vulnerability scanning is enabled
2022-11-09T19:11:29.223+0300    INFO    Secret scanning is enabled
2022-11-09T19:11:29.223+0300    INFO    If your scanning is slow, please try '--security-checks vuln' to disable secret scanning
2022-11-09T19:11:29.223+0300    INFO    Please see also https://aquasecurity.github.io/trivy/v0.34/docs/secret/scanning/#recommendation for
2022-11-09T19:11:32.930+0300    INFO    Detected OS: alpine
2022-11-09T19:11:32.930+0300    INFO    Detecting Alpine vulnerabilities...
2022-11-09T19:11:32.934+0300    INFO    Number of language-specific files: 0
2022-11-09T19:11:32.935+0300    WARN    This OS version is no longer supported by the distribution: alpine 3.3.3
2022-11-09T19:11:32.935+0300    WARN    The vulnerability detection may be insufficient because security updates are not provided

ui (alpine 3.3.3)

Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 1)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
sqlite-libs	CVE-2017-10989	CRITICAL	3.9.2-r1	3.13.0-r1	sqlite: Heap-buffer overflow in the getNodeSize function https://avd.aquasec.com/nvd/cve-2017-10989

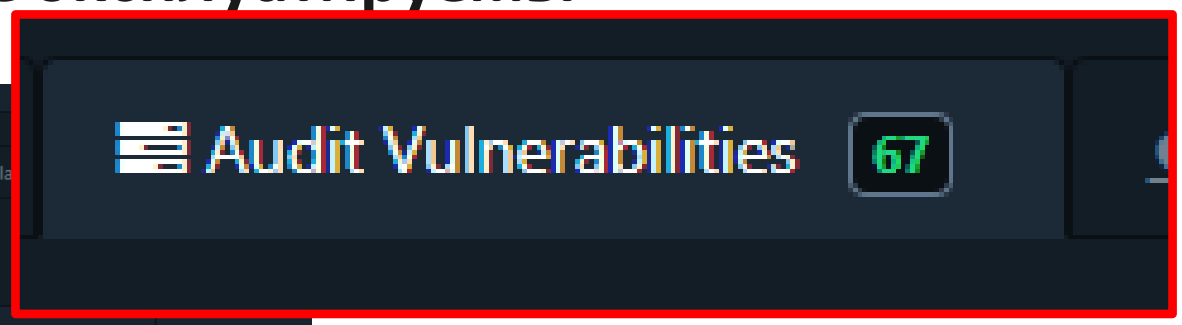
Эти CVE не эксплуатируемы

Components 300 | Services 0 | Dependency Graph 0 | Audit Vulnerabilities 67 | Policy Viola

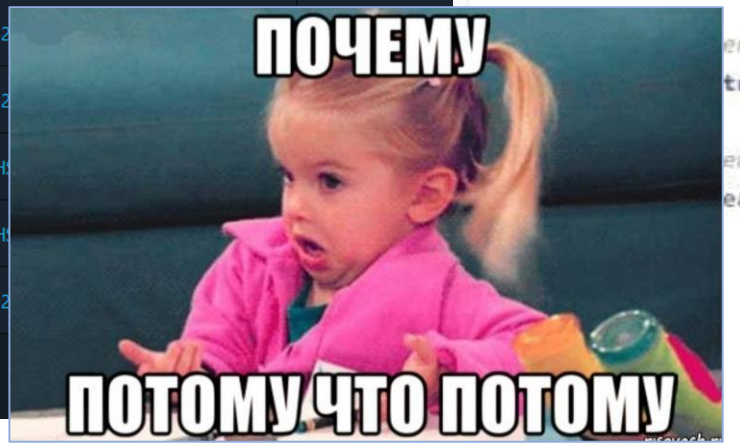
Show suppressed findings

Component	Version	Group	Vulnerability	Severity
esapi	2.0.1	org.owasp.esapi	NVD CVE-2022-23457	Critical
solr-solrj	8.5.1	org.apache.solr	NVD CVE-2021-29943	Critical
spring-beans	5.2.7.RELEASE	org.springframework	NVD CVE-2022-22965	Critical
spring-boot-starter-web	2.3.1.RELEASE	org.springframework.boot	GITHUB GHSA-36p3-wjmg-h94x	Critical
spring-security-core	5.3.3.RELEASE	org.springframework.security	GITHUB GHSA-hh32-7344-cg2f	Critical
spring-web	5.2.7.RELEASE	org.springframework	NVD CVE-2	
spring-web	5.3.21	org.springframework	NVD CVE-2	
spring-webmvc	5.2.7.RELEASE	org.springframework	GITHUB GH	
tomcat-embed-core	9.0.36	org.apache.tomcat.embed	GITHUB GH	
itext	2.1.7	com.lowagie	NVD CVE-2	

ing 1 to 10 of 67 rows 10 rows per page




```
public sealed class JaegerHealthCheck : IHealthCheck
{
    private const string Description = "Проверка работоспс
    private const string HealthCheckName = "Jaeger";
    private readonly Lazy<HttpClient> _httpClient;
    private readonly IHttpClientFactory _clientFactory;

    private readonly IGaspsConfig _config;

eritdoc cref="IHealthCheck.Id" />
tring Id { get; } = HealthCheckName;

eritdoc cref="IHealthCheck.DependencyType" />
ealthDependencyType DependencyType { get; } =
```

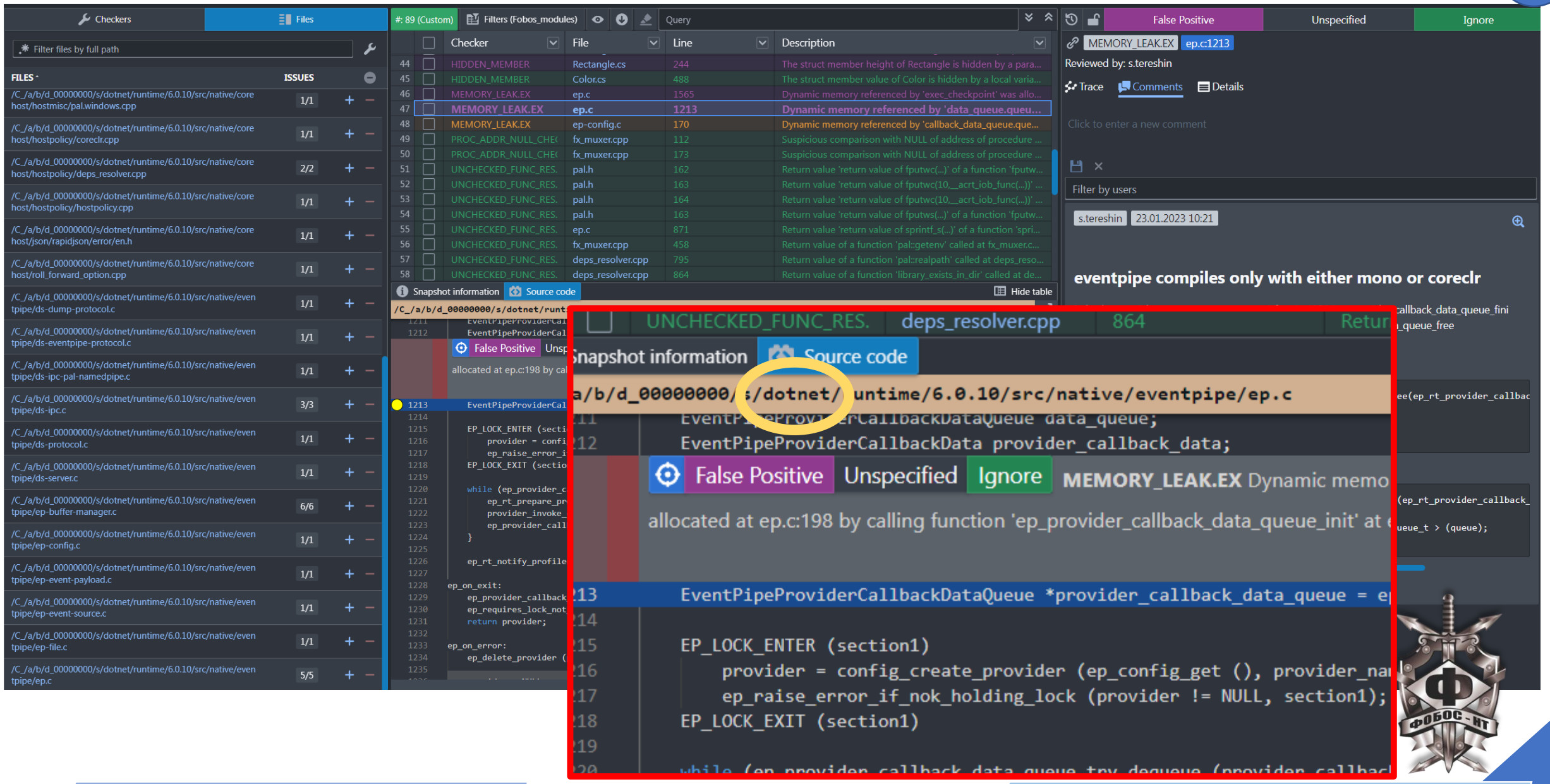


У нас нет интерпретаторов

Perl

Lua

Исследование критических компонент



Определение поверхности атаки

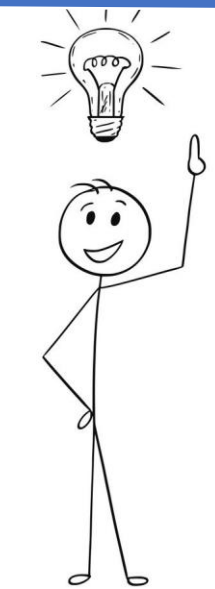
- Не заявлены модули, реализующие функции безопасности.

- Заявлены модули, которые не обрабатывают данные.

- Ошибка определения большого количества ИФБО.

- Не включены модули, стоящие за другими, к которым нет прямого доступа.

Определение поверхности атаки



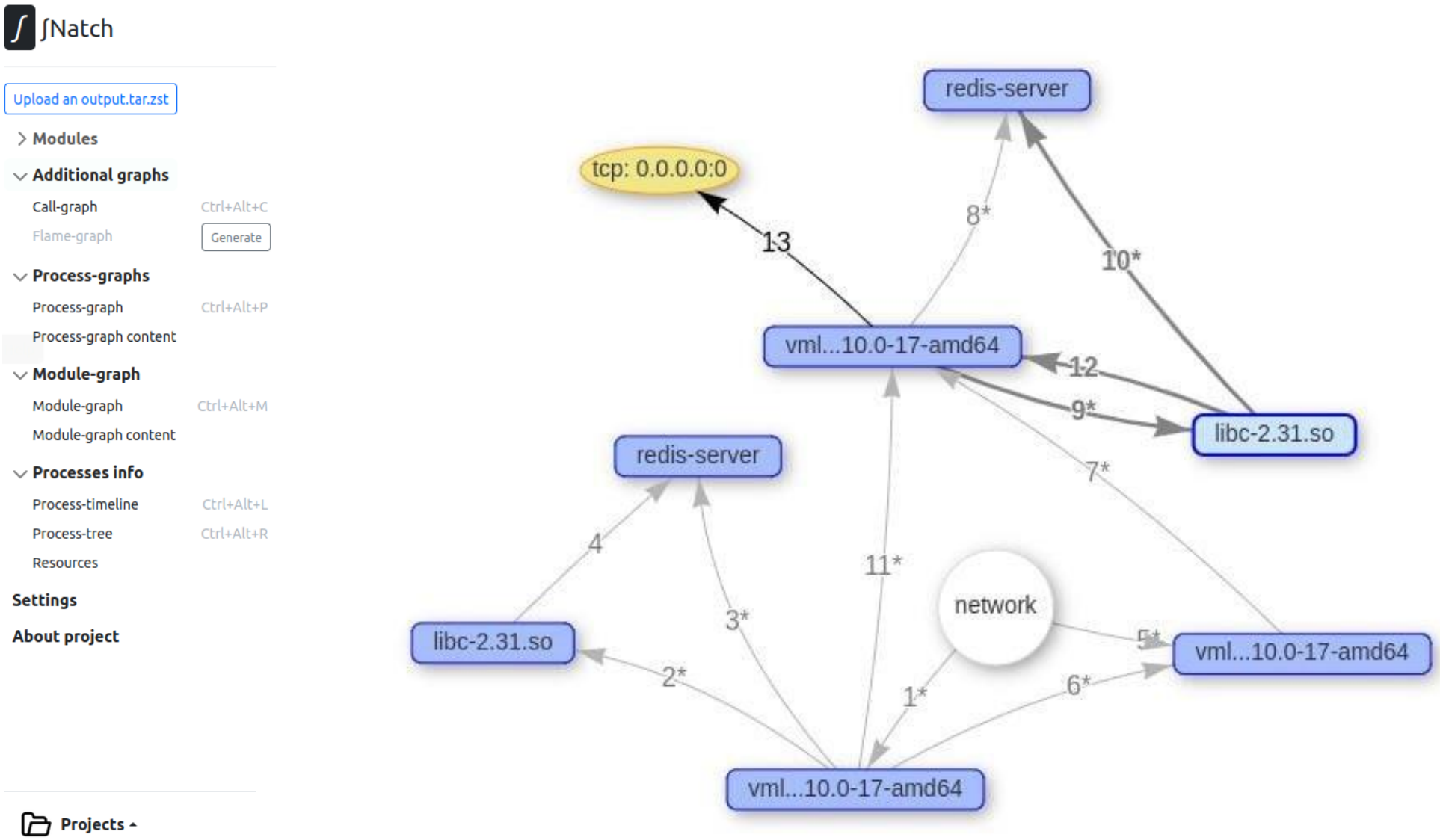
Практики безопасной разработки

- статический анализ;
- использование систем отслеживания известных уязвимостей;
- модульное и функциональное тестирование;
- фаззинг-тестирование;
- выявление побочных взаимодействий со средой функционирования;
- анализ утечек чувствительных данных;
- тестирование на проникновение.

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

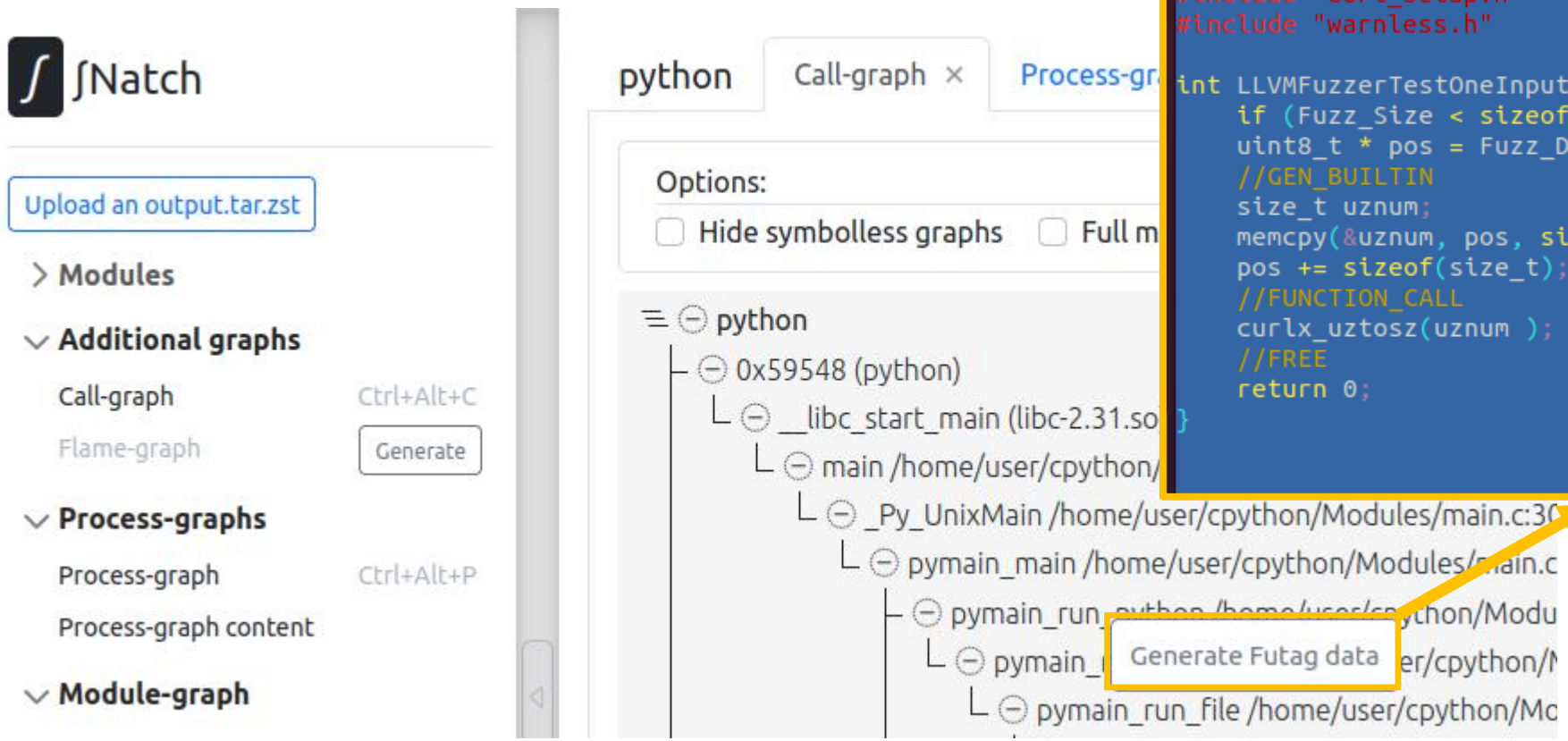
Инструмент для определения поверхности атаки Natch

ИСП РАН



Инструмент для определения поверхности атаки Natch

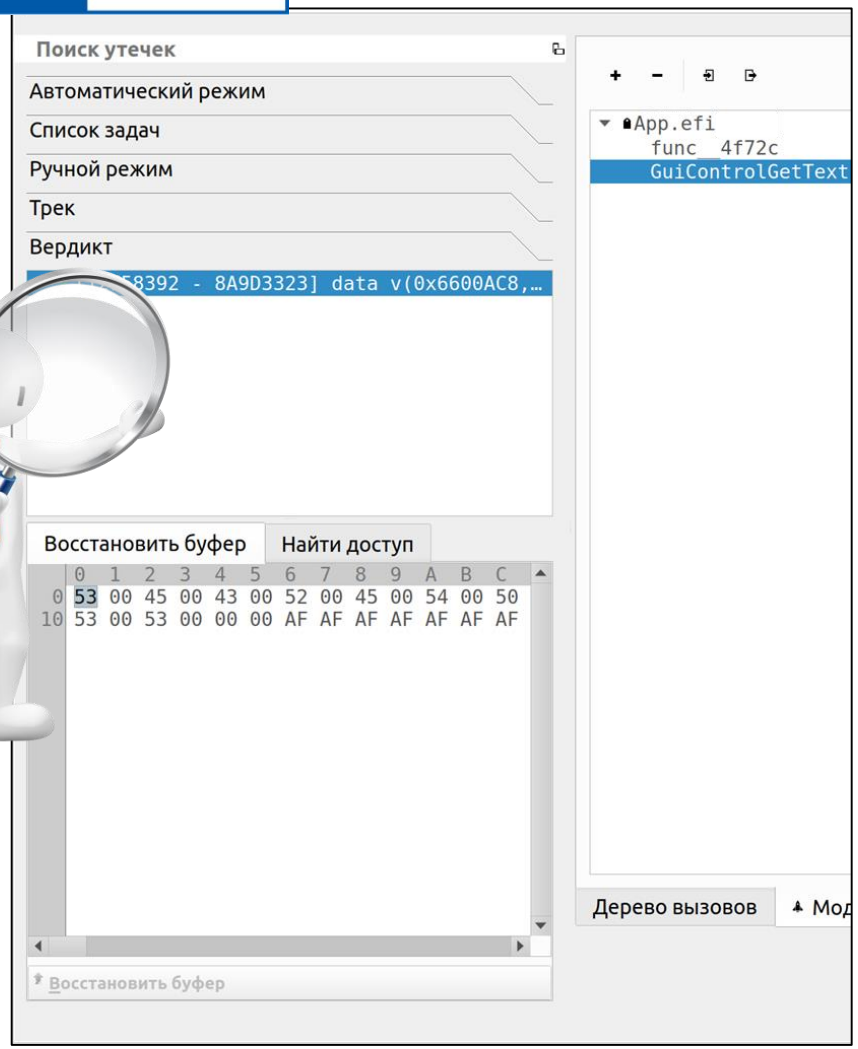
ИСП РАН

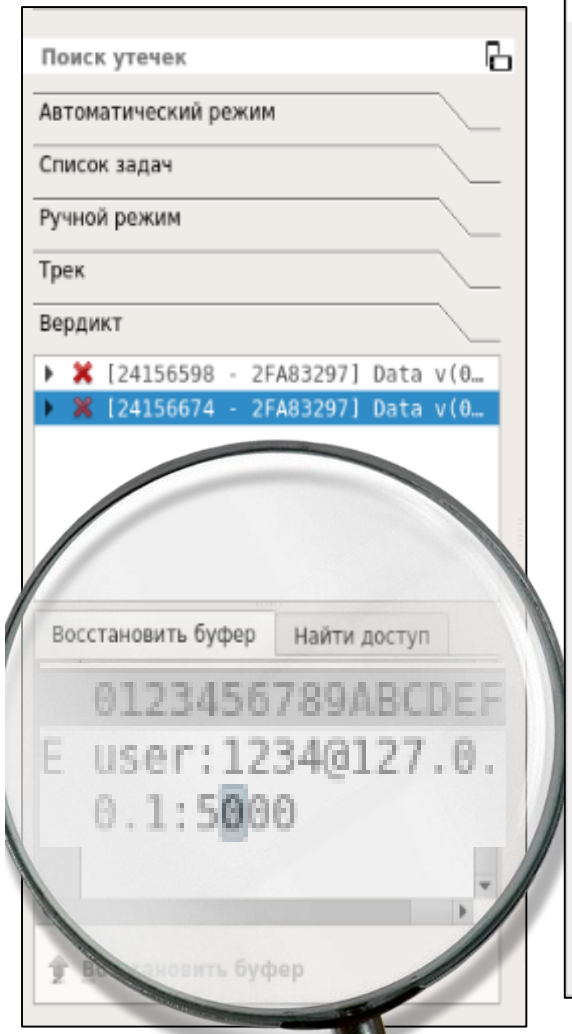


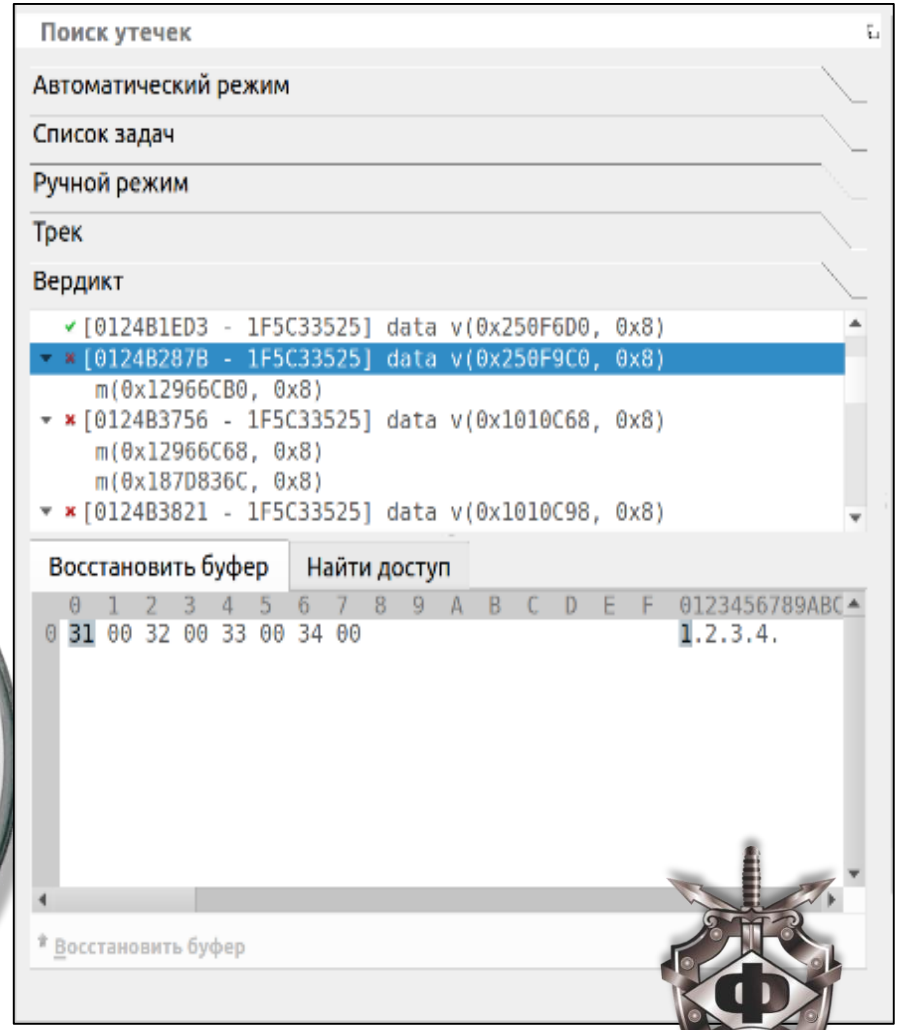

```c
#include <stdio.h>
#include <stddef.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include "curl_setup.h"
#include "warnless.h"

int LLVMFuzzerTestOneInput(uint8_t * Fuzz_Data, size_t Fuzz_Size){
    if (Fuzz_Size < sizeof(size_t)) return 0;
    uint8_t * pos = Fuzz_Data;
    //GEN_BUILTIN
    size_t uznum;
    memcpy(&uznum, pos, sizeof(size_t));
    pos += sizeof(size_t);
    //FUNCTION_CALL
    curlx_uztosz(uznum );
    //FREE
    return 0;
}
```

Блесна: инструмент динамического анализа помеченных данных

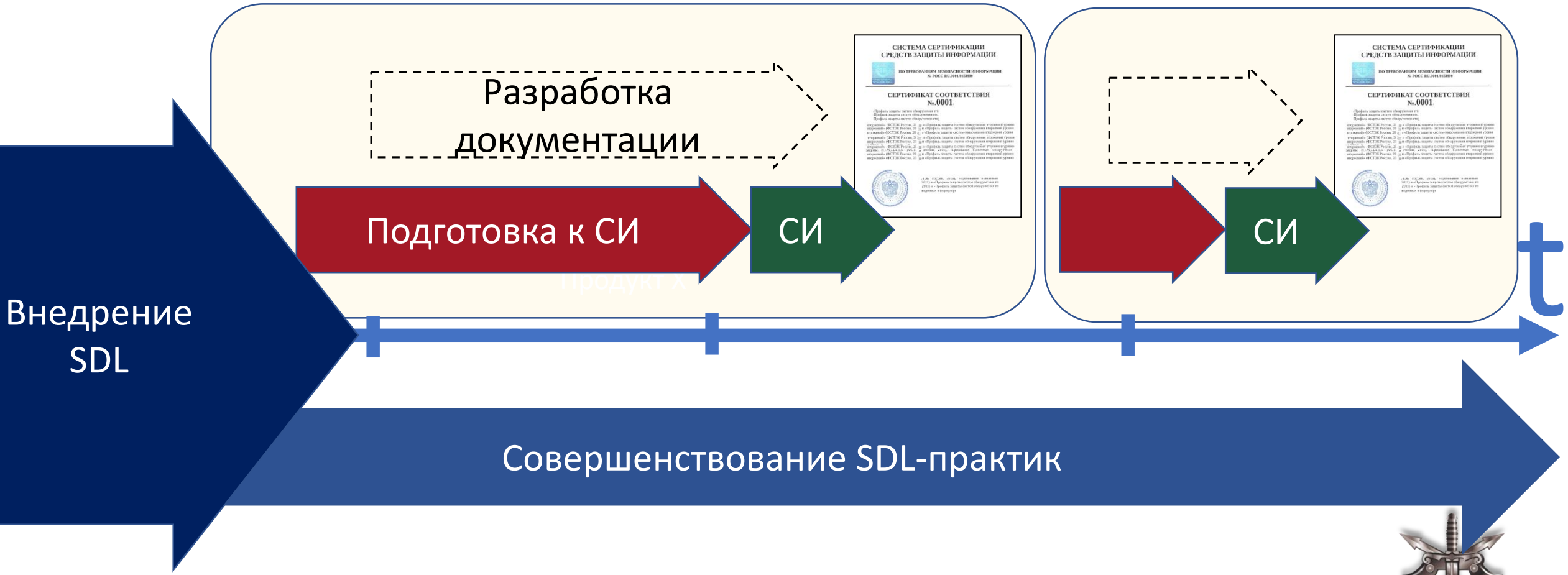
ИСП РАН





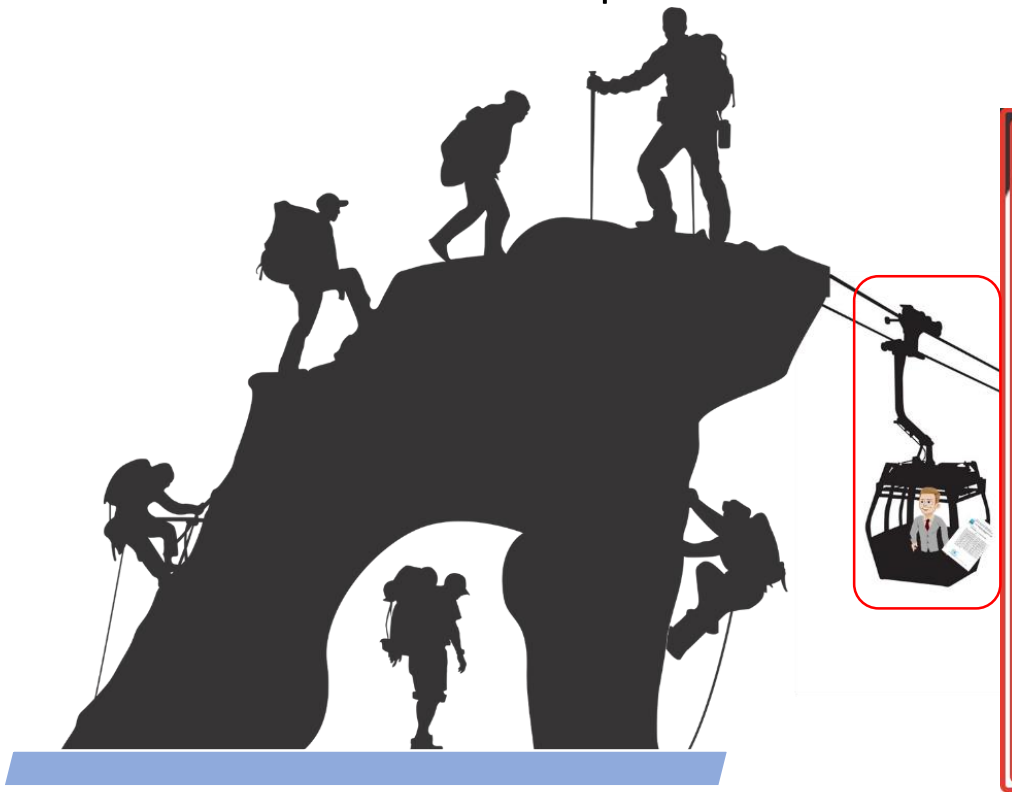


Процесс сертификации СЗИ



Радости

- Изменяется нормативная документация.
- Общение с крутыми специалистами.
- Работа с слаженными SDL командами.
- Предсказуемые сроки сертификации.
- Живое активное сообщество.



Спасибо за внимание!

Борзов Роман Викторович, r.borzov@fobos-nt.ru

Кузнецов Андрей Викторович, a.kuznetcov@fobos-nt.ru

https://fobos-nt.ru