



# SPbSUT)))

**Исследование возможности  
применения технологий  
автоматизации**

**в целях повышения ИБ  
в компьютерных сетях**



**Всегда на связи с будущим!**



# О докладчике

SPbSUT)))

Автор:

**Захаров Денис Артурович,**  
Почти выпускник СПбГУТ,  
Security Engineer,  
Google IT Support Professional Certificate

Дипломный руководитель:

**Ушаков Игорь Александрович**  
к.т.н., доцент кафедры ЗСС



@MisterZurg

**Исследовать возможность применения технологий автоматизации с целью повышения ИБ**

**Рассмотреть:**

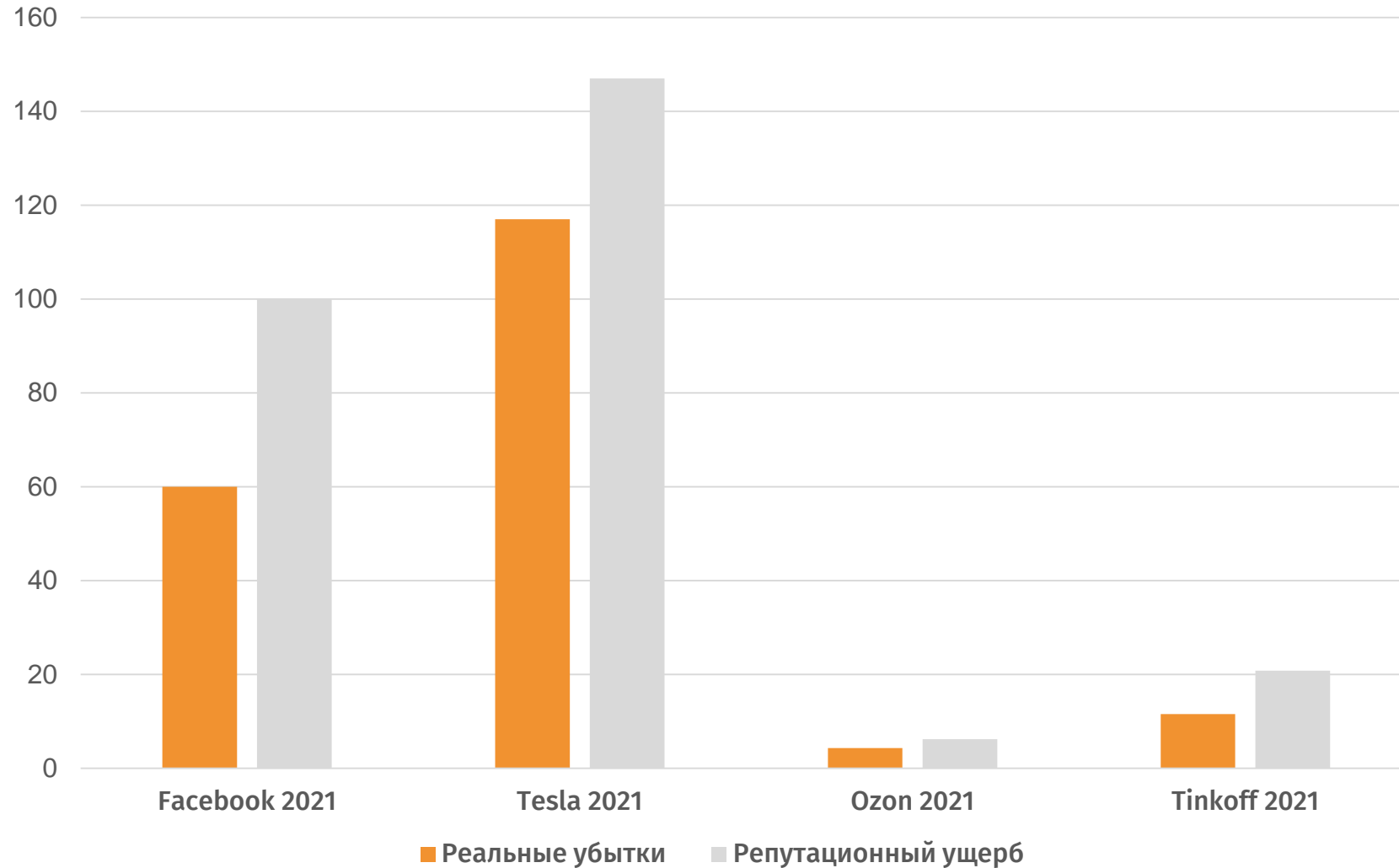
- проблемы предшествующего года в индустрии;
- подходы к разработке ПО;
- угрозы предшествующего года;
- инструменты автоматизации;
- процессы применяемые в организациях.

**Сопроводить этот материал не только теоретической, но в практической частью.**

**Выступить и Защититься на отлично!**

# Актуальность : Потери за 2021

4

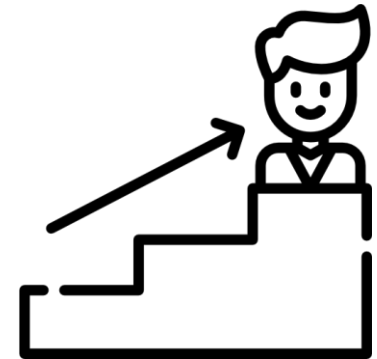


SPbSUT)))

SPbSUT)))

## Автоматизация технических процессов

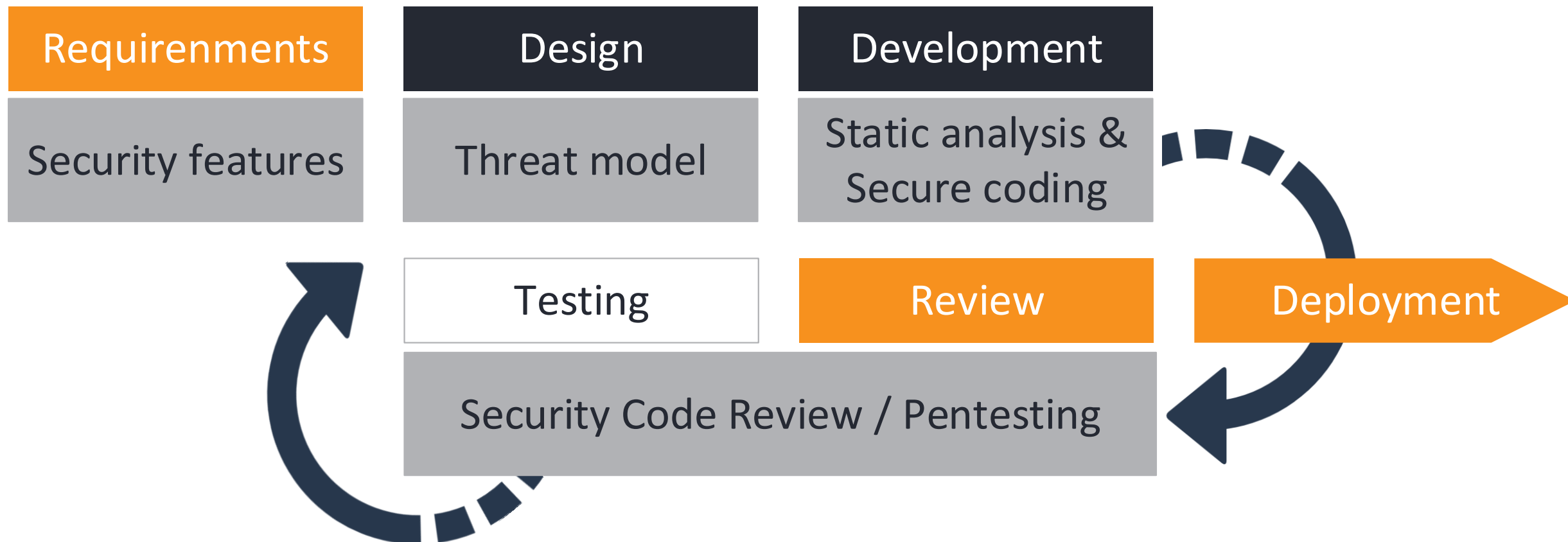
- увеличение объёмов выпускаемой продукции;
- повышение эффективности производственного процесса;
- повышение качества продукции;
- снижение расходов;
- **повышение безопасности;**



# Жизненный цикл программного обеспечения

6





Анализ вариантов развертывания с использованием различных моделей

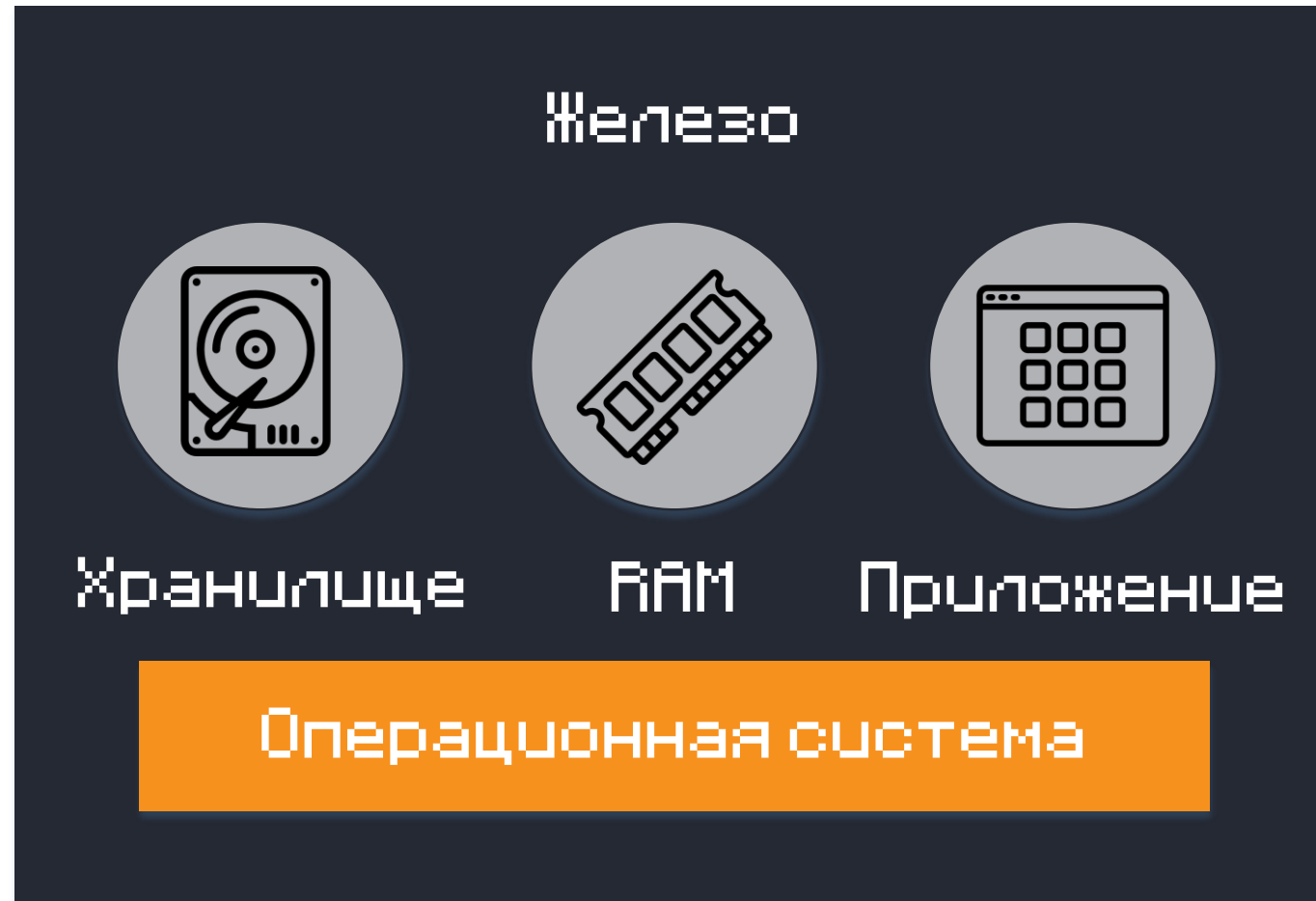
Создание и развертывание приложения

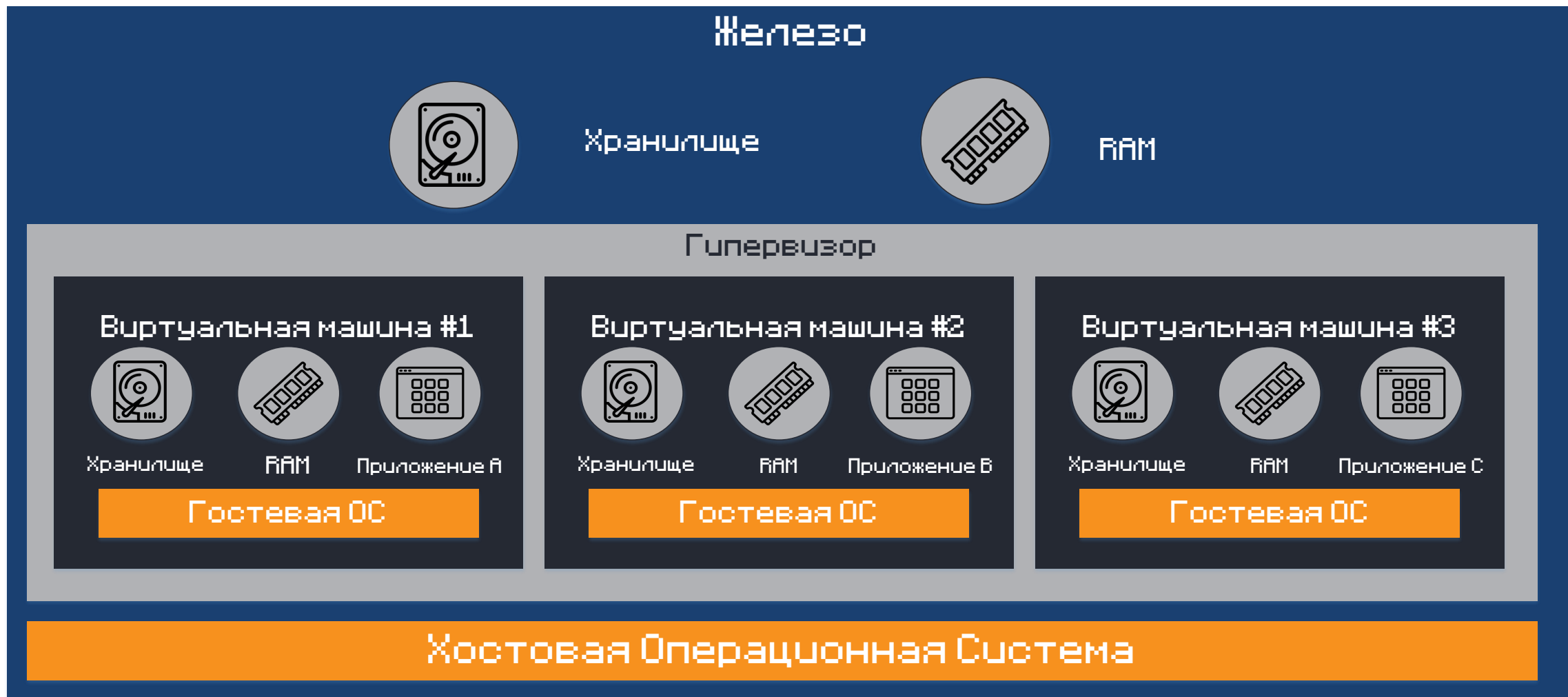
Continuous Integration/Continuous Deployment (CI/CD)

Сети для разработки приложений и безопасности

Безопасность приложений



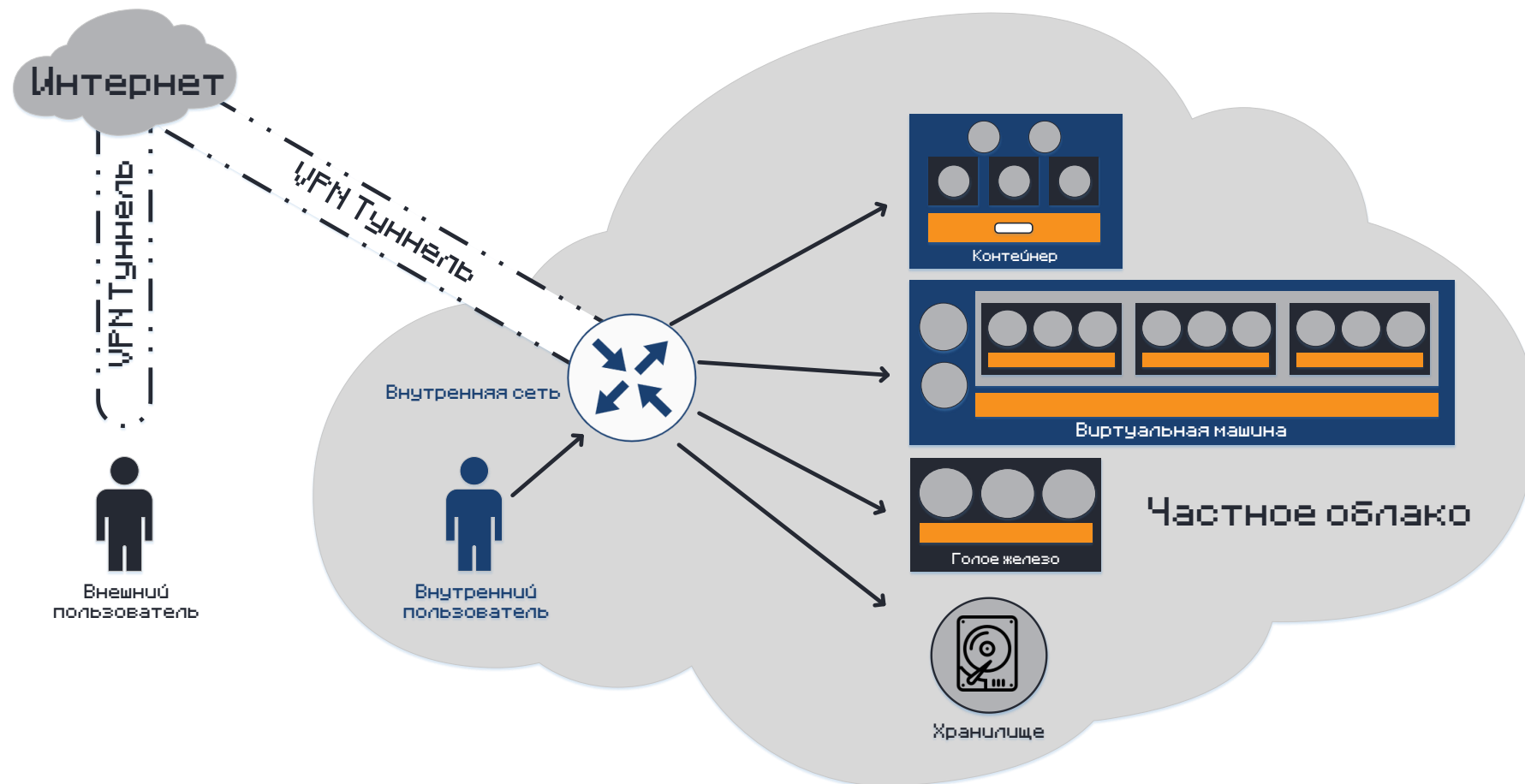


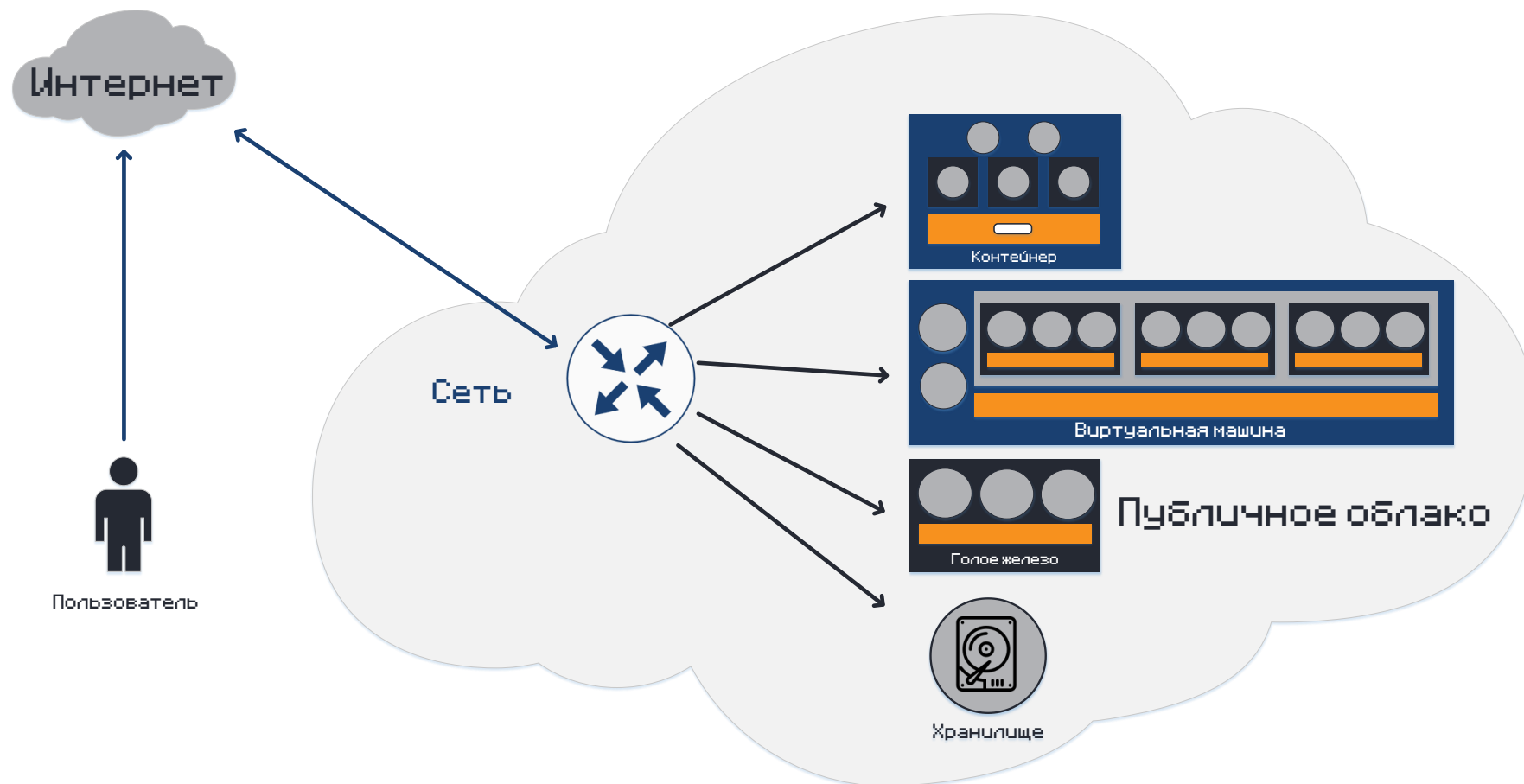


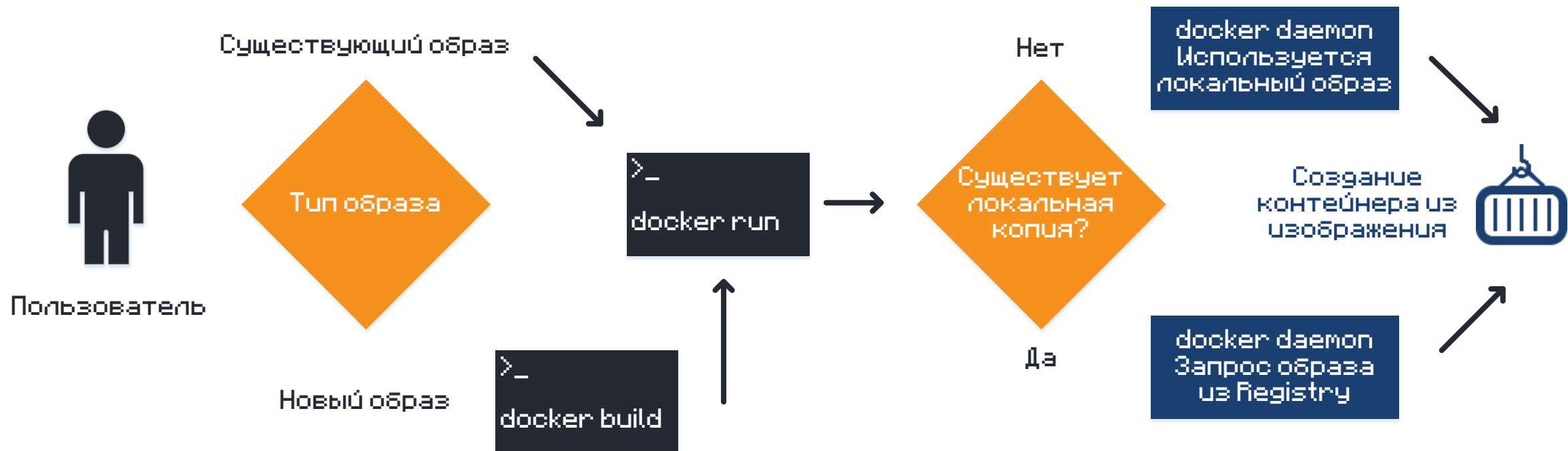
# Инфраструктура на основе контейнеров

11









## Дополнительная безопасность

Запуск небезопасного кода

Изоляция запущенных приложений

Управление контейнерами и их версиями

Производительность

Эффективность



Бесперебойной работа

Интеграция с методологиями Agile

Автоматизированное развертывание

Выпуск функций с меньшими сбоями

Тестирование безопасности

Улучшенное качество

Сокращение среднего времени решения проблемы (MTTR)

Улучшенное время выхода на рынок





CI/CD/CD

Ускорение процесса разработки с пом. автоматизации

Уменьшение ошибок связ. с человеческим фактором

Немедленное Тестирование в том числе и Security

Интеграция с большинством технологий

Повышенная надежность деплоя

Упрощение рабочего процесса

Open Source


# Построение Jenkins Pipeline

18

## Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository.](#)

Owner \*

 MisterZurg ▾

Repository name \*

/ sample-app



Great repository names are short and memorable. Need inspiration? How about **automatic-spork?**

Description (optional)

Изучение CI/CD с помощью GitHub и Jenkins



**Public**

Anyone on the internet can see this repository. You choose who can commit.



**Private**

You choose who can see and commit to this repository.

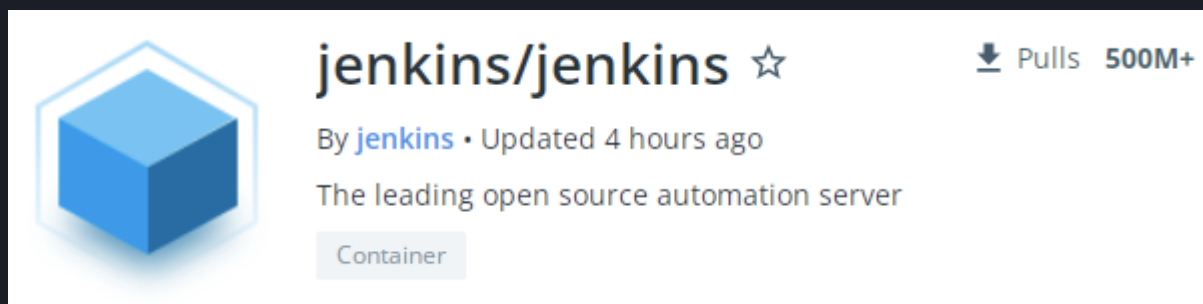
Публикация приложения для интеграции в Jenkins Pipeline

SPbSUT)))

# Построение Jenkins Pipeline

19

```
devasc@labvm:~/labs/devnet-src/jenkins/sample-app$ docker pull jenkins/jenkins
Using default tag: latest
latest: Pulling from jenkins/jenkins
...
Digest: sha256:f1058cadd535b238c80f49a2a7b0a9de71a82bb58d642472eba1f40258dc189
Status: Downloaded newer image for jenkins/jenkins:latest
docker.io/jenkins/jenkins:latest
devasc@labvm:~/labs/devnet-src/jenkins/sample-app$
```



Установка Сервера Jenkins

SPbSUT)))

# Построение Jenkins Pipeline

20

## New personal access token

Personal access tokens function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to [authenticate to the API over Basic Authentication](#).

### Note

Jenkins BuildAppJob Token

What's this token for?

### Expiration \*

7 days



The token will expire on Wed, May 11 2022

### Select scopes

Scopes define the access for personal tokens. [Read more about OAuth scopes](#).







- |   |                                      |
|---|--------------------------------------|
| <input checked="" type="checkbox"/> repo            | Full control of private repositories |
| <input checked="" type="checkbox"/> repo:status     | Access commit status                 |
| <input checked="" type="checkbox"/> repo_deployment | Access deployment status             |
| <input checked="" type="checkbox"/> public_repo     | Access public repositories           |
| <input checked="" type="checkbox"/> repo:invite     | Access repository invitations        |
| <input checked="" type="checkbox"/> security_events | Read and write security events       |
| <hr/>   |                                      |
| <input checked="" type="checkbox"/> workflow        | Update GitHub Action workflows       |

Генерация API токена

SPbSUT)))

# Построение Jenkins Pipeline

21

S	W	Name ↓	Last Success	Last Failure	Last Duration	
		BuildAppJob	37 min <a href="#">#2</a>	N/A	5 sec	
		TestAppJob	N/A	N/A	N/A	





```
# Execute shell  
bash ./sample-app.sh
```

Код собирающей джобы

SPbSUT)))

# Построение Jenkins Pipeline

22

S	W	Name ↓	Last Success	Last Failure	Last Duration
		BuildAppJob	12 sec <a href="#">#6</a>	N/A	3.9 sec 
		TestAppJob	2.5 sec <a href="#">#4</a>	1 min 12 sec <a href="#">#3</a>	1.1 sec 

```
# Execute shell
if curl http://172.17.0.1:5050/ | grep "Ты заходишь на меня с 172.17.0.1"; then
    exit 0
else
    exit 1
fi
```

Код тестирующей джобы

SPbSUT)))

Enter an item name

» *Required field*



## Freestyle project

This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.



## Pipeline

Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

# Построение Jenkins Pipeline

24

```
node {  
    stage('Preparation') {  
        catchError(buildResult: 'SUCCESS') {  
            sh 'docker stop samplerunning'  
            sh 'docker rm samplerunning'  
        }  
    }  
    stage('Build') {  
        build 'BuildAppJob'  
    }  
    stage('Results') {  
        build 'TestAppJob'  
    }  
}
```

Скрипт описывающий пайплайн

SPbSUT)))



## Pipeline SamplePipeline



Recent Changes

### Stage View

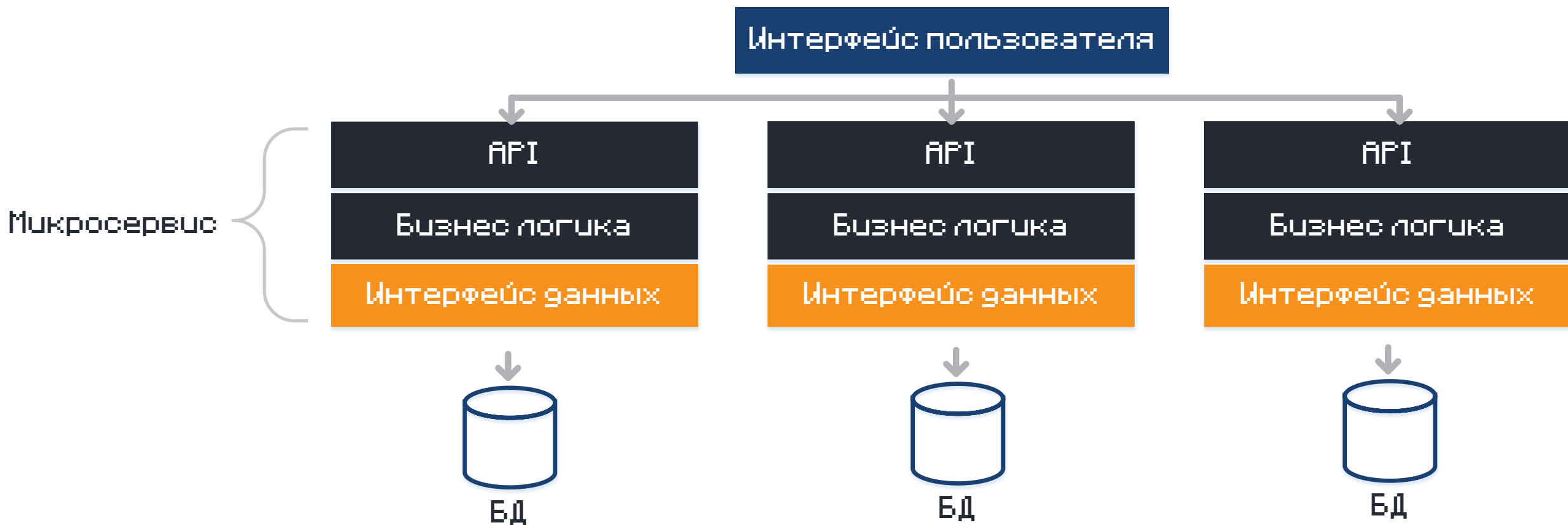
Average stage times:  
(Average full run time: ~32s)

	Preparation	Build	Results
	13s	8s	7s
#1 May 04 22:52 No Changes	13s	8s	7s

Результат запуска пайплайна

SPbSUT)))

- **Broken Access Control;**
- **Cryptographic Failures;**
- **Injection;**
- Insecure Design;
- **Security Misconfiguration;**
- **Vulnerable and Outdated Components;**
- **Identification and Authentication Failures;**
- **Software and Data Integrity Failures;**
- **Security Logging and Monitoring Failures;**
- Server-Side Request Forgery;



# Что делают для нас инструменты автоматизации?

28

Упрощение и стандартизация;

Ускорение разработки с помощью готовых функций;

Облегчение повторного использования;

Разделение проблем;

Повышение безопасности;


Обнаружение и управление устройствами;

Сокращение расходов;

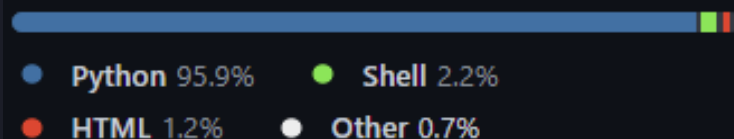
# Материалы представлены на GitHub

SPbSUT)))



 <b>MisterZurg</b> Исправлены пути :/	3c3a791 5 days ago	🕒 5 commits
📁 Laboratory	Исправлены пути :/	5 days ago
📁 Packet-Tracer-Activities	Добалена куча Readme с lab-flow!	5 days ago
📁 Projects	Добалена куча Readme с lab-flow!	5 days ago
📁 Resources	Добалена куча Readme с lab-flow!	5 days ago
📄 LICENSE	Initial commit	13 days ago
📄 README.md	Исправлены пути :/	5 days ago

## Languages



## 26: Лабораторные

SPbSUT)))

Установка виртуальной лабораторной среды

Знакомство с Linux

Знакомство с Python

Инструменты разработки на языке Python

КВ ПО с помощью Git

Классы в Python

Unit-тестирование на Python

Парсинг различных типов данных

Rest API с помощью API Simulator и Postman

Интеграция REST API и Python приложения

Инструменты для устранения неполадок в сети

Исследование простой

Исследование сетевых протоколов

Сравнение CLI и SDN контроллера управления сетью

Сравнение CLI и SDN контроллера

Сборка веб-приложения в Docker контейнере

Построение CI/CD с помощью Jenkins

Исследование эволюции парольных систем

Установка CSR1000v VM

Ansible для резервного копирования и настройки устройства

Ansible для автоматизации установки Веб-сервера


Автоматизированное тестирование с помощью pyATS и Genie

Исследование YANG моделей

NETCONF для доступа к устройству

RESTCONF для доступа к устройству

Python для управления Webex Teams

 **MisterZurg** Добавлена куча Readme с lab-flow!

Latest commit b562c4a 25 days ago [History](#)

👤 1 contributor

⋮ 402 lines (345 sloc) 38.2 KB

<> 📄 Raw Blame 🖨️ 📋 ✎ 🗑️

## Использование Ansible для резервного копирования и настройки устройства

---

### Цель лабораторной работы:

- Часть 1: Запуск виртуальных машин DEVASC и CSR1000v
- Часть 2: Настройка Ansible
- Часть 3: Ansible для резервного копирования конфигурации
- Часть 4: Ansible для настройки устройства

```
---
- name: AUTOMATIC BACKUP OF RUNNING-CONFIG
  hosts: CSR1kv
  gather_facts: false
  connection: local

  tasks:
    - name: DISPLAYING THE RUNNING-CONFIG
      ios_command:
        commands:
          - show running-config
      register: config

    - name: SAVE OUTPUT TO ./backups/
      copy:
        content: "{{ config.stdout[0] }}"
        dest: "backups/show_run_{{ inventory_hostname }}.txt"
```



# Ansible для backup'ов и настройки устройств

33

```
devasc@labvm:~/labs/devnet-src/ansible/ansible-csr1000v$ ansible-playbook backup_cisco_router_playbook.yaml -i hosts

PLAY [AUTOMATIC BACKUP OF RUNNING-CONFIG] *****
*****

TASK [DISPLAYING THE RUNNING-CONFIG] *****
*****
ok: [CSR1kv]

TASK [SAVE OUTPUT TO ./backups/] *****
*****
changed: [CSR1kv]

PLAY RECAP *****
*****
CSR1kv                : ok=2    changed=1    unreachable=0    failed=0
                       skipped=0    rescued=0    ignored=0

devasc@labvm:~/labs/devnet-src/ansible/ansible-csr1000v$
```

# Ansible для backup'ов и настройки устройств

34

```
devasc@labvm:~/labs/devnet-src/ansible/ansible-csr1000v$ cat backups/show_run_CSR1kv.txt
```

```
Building configuration...
```

```
Current configuration : 3915 bytes
```

```
!
```

```
! Last configuration change at 20:54:52 UTC Mon May 9 2022
```

```
!
```

```
version 16.9
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
platform qfp utilization monitor load 80
```

```
no platform punt-keepalive disable-kernel-core
```

```
platform console virtual
```

```
!
```

```
hostname CSR1kv
```

```
!
```

```
<ВЫВОД опущен>
```

SPbSUT)))

# Ansible для backup'ов и настройки устройств

35

```
devasc@labvm:~/labs/devnet-src/ansible/ansible-csr1000v$ ansible-playbook -v cisco_router_ipv6_
config_playbook.yaml
Using /home/devasc/labs/devnet-src/ansible/ansible-csr1000v/ansible.cfg as config file

PLAY [CONFIGURE IPv6 ADDRESSING] *****

TASK [SET IPv6 ADDRESS] *****
changed: [CSR1kv] => {"ansible_facts": {"discovered_interpreter_python": "/usr/bin/python3"}, "
banners": {}, "changed": true, "commands": ["interface GigabitEthernet1", "ipv6 address 2001:db
8:acad:1::1/64", "ipv6 address fe80::1:1 link-local"], "updates": ["interface GigabitEthernet1"
, "ipv6 address 2001:db8:acad:1::1/64", "ipv6 address fe80::1:1 link-local"]}

TASK [SHOW IPv6 INTERFACE BRIEF] *****
ok: [CSR1kv] => {"changed": false, "stdout": ["GigabitEthernet1      [up/up]\n      FE80::1:1\n
2001:DB8:ACAD:1::1"], "stdout_lines": [["GigabitEthernet1      [up/up]", "      FE80::1:1", "
2001:DB8:ACAD:1::1"]]}

TASK [SAVE OUTPUT ./ios_configurations/] *****
changed: [CSR1kv] => {"changed": true, "checksum": "60784fbaae4bd825b7d4f121c450effe529b553c",
"dest": "ios_configurations/IPv6_output_CSR1kv.txt", "gid": 900, "group": "devasc", "md5sum": "
56e879f15e6e776cf131cec5abfc1886", "mode": "0664", "owner": "devasc", "size": 67, "src": "/home
/devasc/.ansible/tmp/ansible-tmp-1652131158.3335166-4547-279519168591363/source", "state": "fil
e", "uid": 900}

PLAY RECAP *****
CSR1kv                : ok=3    changed=2    unreachable=0    failed=0    skipped=0    res
cued=0    ignored=0

devasc@labvm:~/labs/devnet-src/ansible/ansible-csr1000v$ █
```

SPbSUT)))

```
devasc@labvm:~/labs/devnet-src/ansible/ansible-csr1000v$ cat  
ios_configurations/IPv6_output_CSR1kv.txt  
GigabitEthernet1 [up/up]  
    FE80::1:1  
    2001:DB8:ACAD:1::1  
devasc@labvm:~/labs/ansible-csr1000v/ios_configurations$
```

Формирование команды

Формирование Agile команды

Социальное программирование

Автоматизированное тестирование и  
развертывание программного обеспечения

Программирование и автоматизация сети

# Прил 3: Много Дополнительной теории

SPbSUT)))

, не вошедшей в основную часть дипломной работы. 200+ стр

Version Control Systems and Git

Canary и Blue/Green деплои

Ansible, Puppet, Chef, pyATS примеры

Switching

Virtual LANs (VLANs)

Internetwork Layer

Сетевые устройства

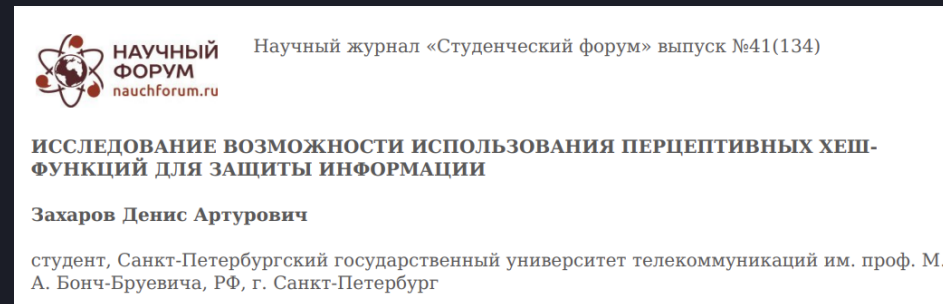
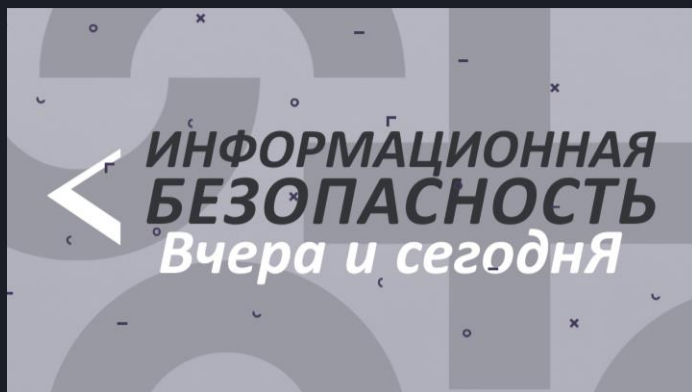
NETCONF

RESTCONF

...

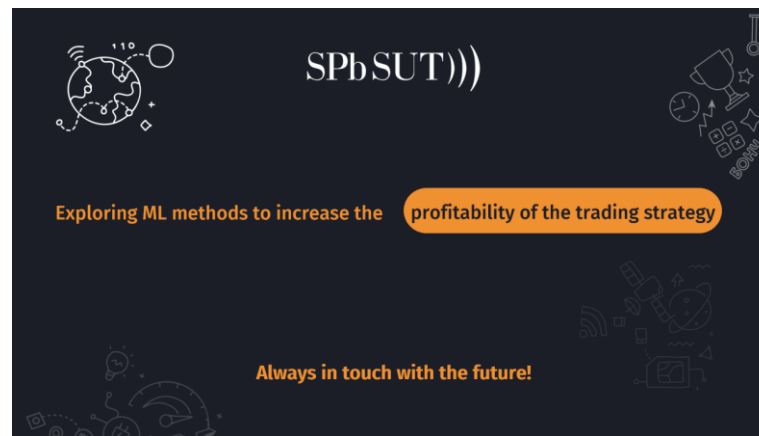
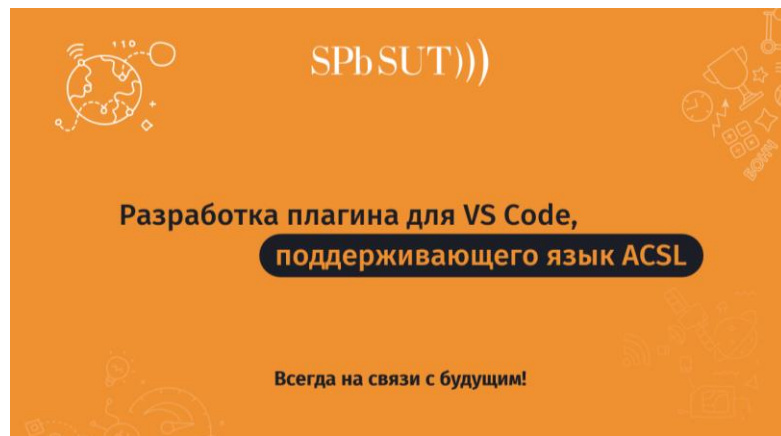
# До 2022 года

SPbSUT)))



# 2022 год

# SPbSUT)))





# ИТОГИ:

STUDENT SPRING — 2019 «Information security yesterday and today»;

STUDENT SPRING — 2020 «Simulation model of a delta codec for an RF signal»;

NAUCHFORUM — 2020 «Investigation of the possibility of using perceptual hash functions to protect information»;

STUDENT SPRING — 2021 «Researching approaches to secure software development»;

RESEARCH — 2022 «Exploring ML methods to increase the profitability of the trading strategy»;

STUDENT SPRING — 2022 «Information Security in Automating vSphere Infrastructure Deployment using PowerCLI»;

**Bachelors Diploma — 2022 «Exploring the use of automation technologies to improve information security in computer networks»**

?

?

?

?

?

?

Q  
:/

?

?

?

?

?

?

# Используемые источники

Глобальный сбой в работе Facebook, Instagram и WhatsApp продолжался более 5 часов, DNS Facebook заработал / [Electronic resource] /

Рекомендации по обеспечению безопасности для цепочки поставок программного обеспечения / [Electronic resource] / Access mode : <https://docs.microsoft.com/ru-ru/nuget/concepts/security-best-practices>

2021 Facebook outage // [Electronic resource]. – URL: [https://en.wikipedia.org/wiki/2021\\_Facebook\\_outage](https://en.wikipedia.org/wiki/2021_Facebook_outage)

Docker Documentation [Electronic resource] <https://docs.docker.com/>

Jenkins User Documentation [Electronic resource] <https://www.jenkins.io/doc/>

Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides. Design Patterns: Elements of Reusable Object-Oriented Software: [Text] / / – 1 Edition. – 1994. – 395 с.

Niall Murphy, Chris Jones, Betsy Beyer, Jennifer Petoff. Site Reliability Engineering: How Google Runs Production Systems: [Text] / – 1 Edition. – 2016. – 550 с.

Jennifer Davis, Ryn Daniels. Effective DevOps: Building a Culture of Collaboration, Affinity, and Tooling at Scale: [Text] / – 1 Edition. – 2016. – 625 с.

DevOps ЗДОРОВОГО ЧЕЛОВЕКА / Все пути ведут в КУБЕРНЕТЕС / Интервью с Дмитрием Столяровым // [Electronic resource]. – URL: [https://www.youtube.com/watch?v=htm12lYKDU&ab\\_channel=%D0%90%D0%B9%D0%A2%D0%B8%D0%91%D0%BE%D1%80%D0%BE%D0%B4%D0%B0](https://www.youtube.com/watch?v=htm12lYKDU&ab_channel=%D0%90%D0%B9%D0%A2%D0%B8%D0%91%D0%BE%D1%80%D0%BE%D0%B4%D0%B0)

OWASP Top Ten [Electronic resource]. – URL: <https://owasp.org/www-project-topten/>

Тестируем на проде: Canary Deployment [Electronic resource]. – URL: <https://habr.com/ru/company/oleg-bunin/blog/493026/>

Сине-зеленый деплой // [Electronic resource]. – URL: <https://habr.com/ru/post/309832/>

Обеспечиваем безопасность в гибкой разработке и CI/CD <https://habr.com/ru/company/southbridge/blog/525208/>



# SPbSUT)))

**Благодарю  
за ваше время!**

**Denis Zakharov**  
2022

