Управление уязвимостями в новых реалиях

Vulns.io VM

Новые реалии – зарубежные VM-решения

Qualys
VMDR
tenable
Nessus vulnerability scanner
tenable.io
RAPID7
metasploit
nexpose
TRIPWIRE IP360
GFI LanGuard

2017 2018 2019 2020 2021 2022 2023

Новые реалии – зарубежные VM-решения ушли из РФ

2017 2018 2019 2020 2021 2022 2023

фродекс

Новые реалии – рост кибератак на российские компании

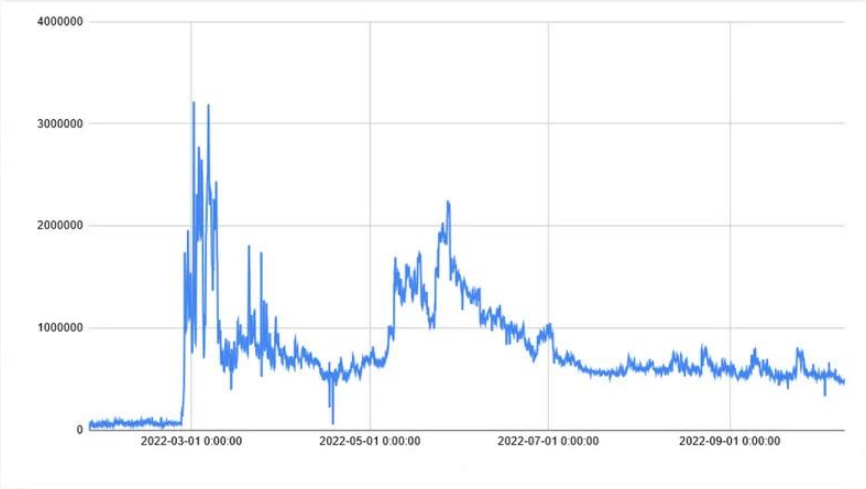
в 15 раз
рост количества атак

HTTP-флуд
самый распространенный вид атак

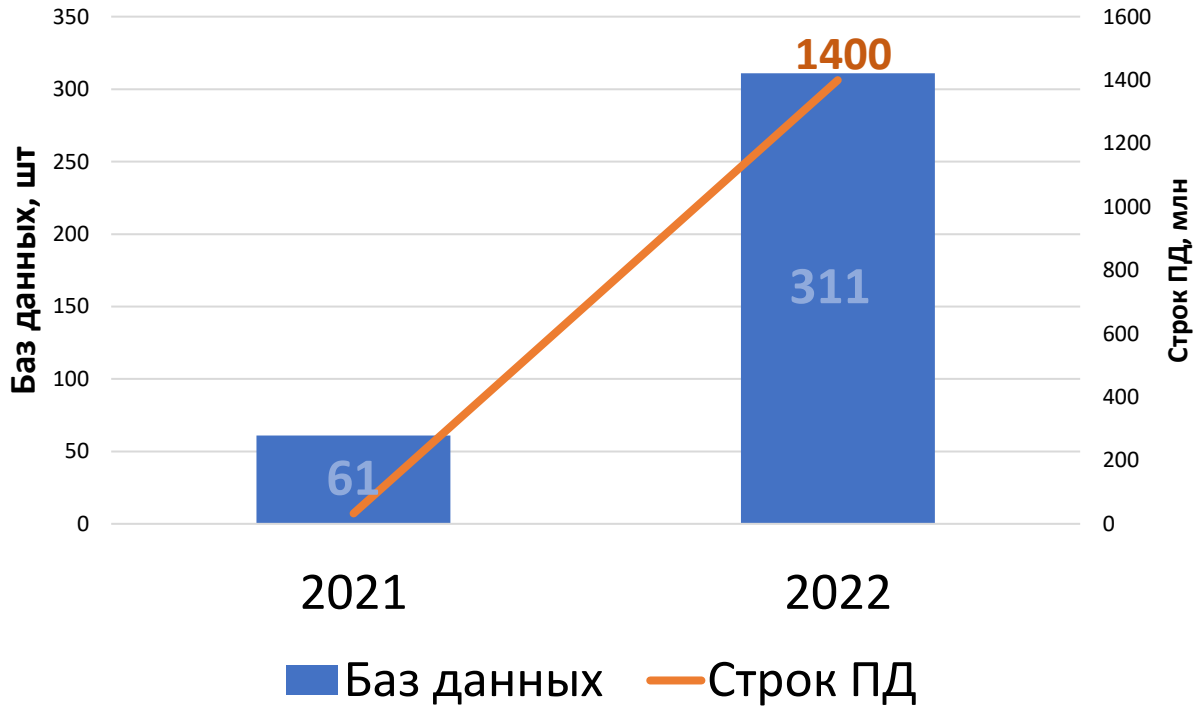
Финансовый сектор
лидер по числу атак

Несколько недель
продолжительность атак

Интенсивность DDoS-атак на российские компании с февраля 2022 года



Динамика утечек персональных данных компаний за 2021-2022 г.*



*По данным пресс-релиза компании GroupIB (https://www.group-ib.ru/media-center/press-releases/database-2022/)

2022 — 2023

фродекс

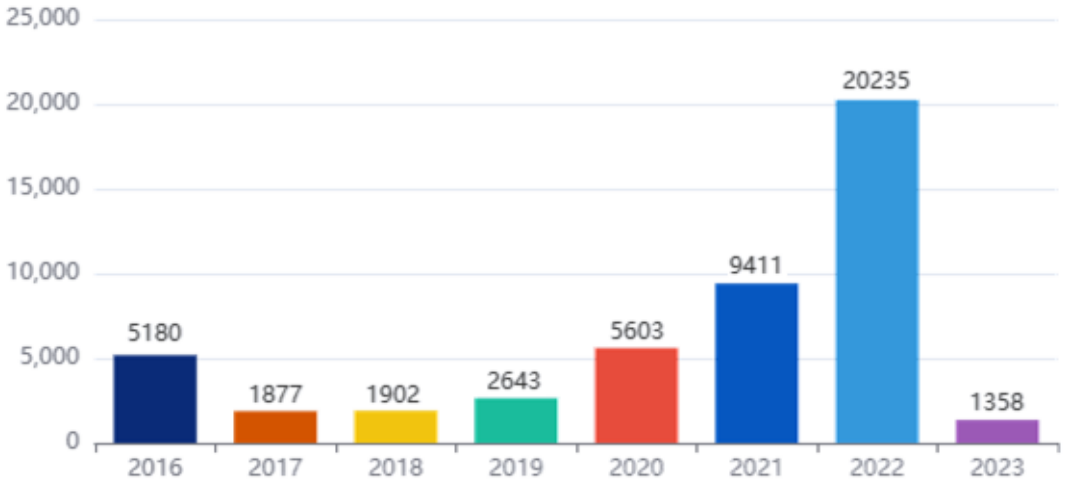
Новые реалии – развитие российского ПО

РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

16 201
Включено ПО в Реестр

5 485
Правообладателей

Количество заявлений на включение ПО в Реестр за период 2016-2023 гг.



Переход на отечественные операционные системы

ASTRA LINUX®

РЕДОС

alt linux
ALT LINUX TEAM

ROSA

ОСНОВА

АВРОРА

СТРЕЛЕЦ
ОПЕРАЦИОННАЯ СИСТЕМА ОБЩЕГО НАЗНАЧЕНИЯ

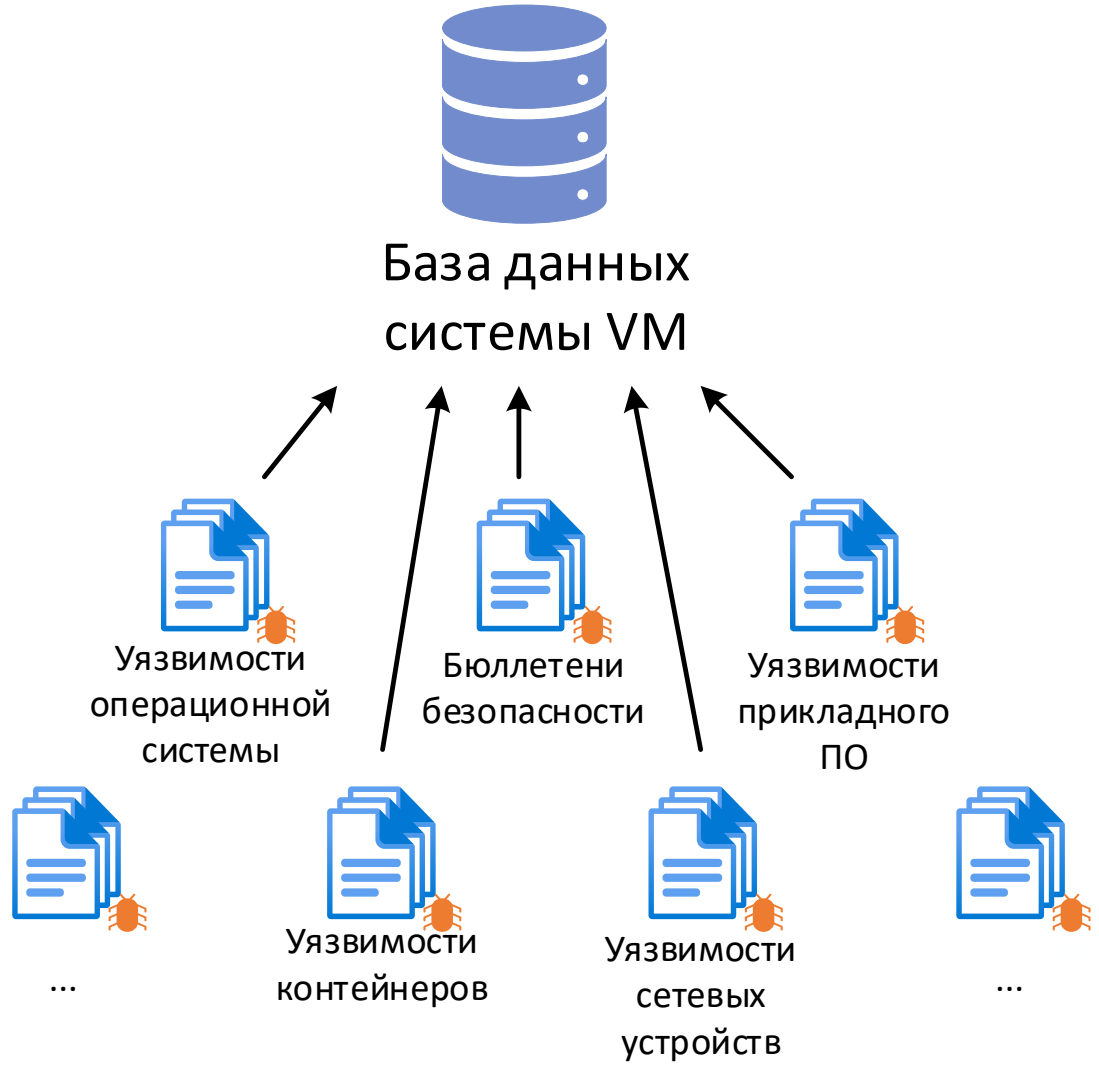
ФССП России
GosLinux

UB Linux

2022 — 2023

фродекс

Фундамент VM-системы



А что с данными? Западный IT-сегмент

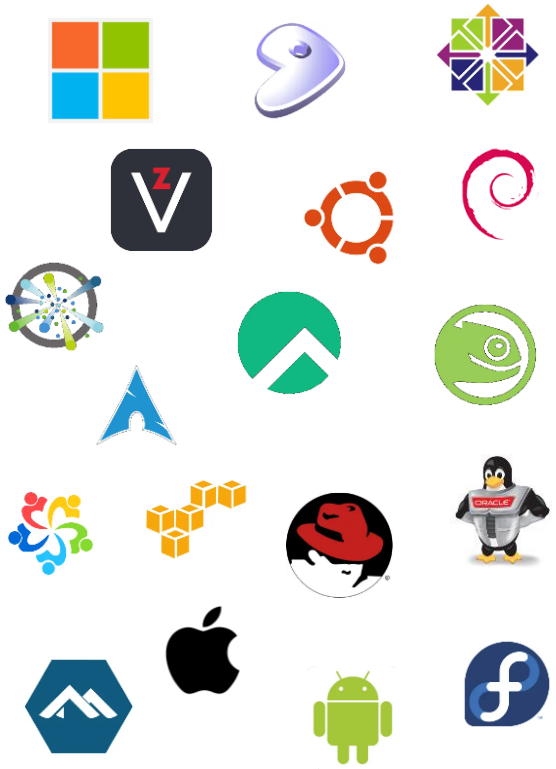
Государственный источник

NIST NATIONAL VULNERABILITY DATABASE NVD

NVD Contains

CVE Vulnerabilities	206541
Checklists	602
US-CERT Alerts	249
US-CERT Vuln Notes	4487
OVAL Queries	10286
CPE Names	1017955

Операционные системы



Программное обеспечение

фродекс

А что с данными? Западный IT-сегмент

Государственный источник

NIST NATIONAL VULNERABILITY DATABASE NVD

NVD Contains

CVE Vulnerabilities	206541
Checklists	602
US-CERT Alerts	249
US-CERT Vuln Notes	4487
OVAL Queries	10286
CPE Names	1017955

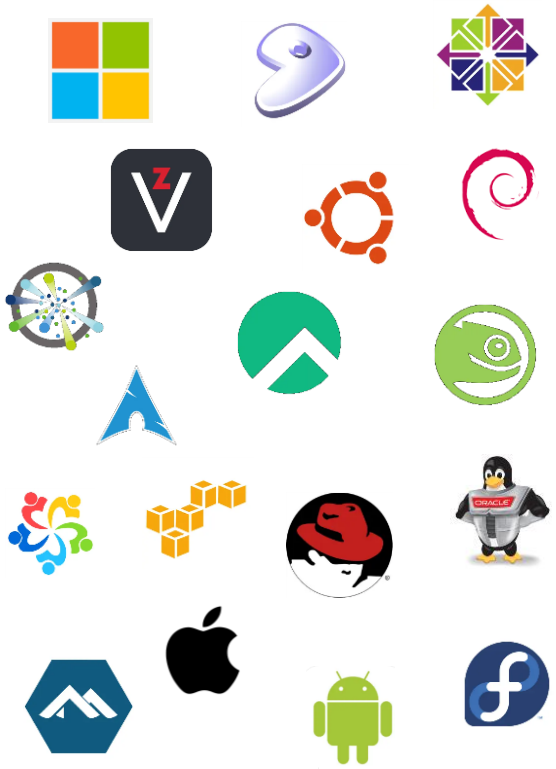
Стандарты описания уязвимостей

CVE Common Vulnerabilities and Exposures

CVSS

OVAL

Операционные системы



Программное обеспечение

фродекс

А что с данными? Западный IT-сегмент

Государственный источник

NIST NATIONAL VULNERABILITY DATABASE NVD

NVD Contains

CVE Vulnerabilities	206541
Checklists	602
US-CERT Alerts	249
US-CERT Vuln Notes	4487
OVAL Queries	10286
CPE Names	1017955

Стандарты описания уязвимостей

CVE Common Vulnerabilities and Exposures · CVSS · OVAL

Операционные системы

Программное обеспечение

фродекс

А что с данными? Российский IT-сегмент

Государственный источник

БДУ ФСТЭК

- Дата создания: март 2015
- Уязвимостей: **44 836**
- Вендоров ПО: **1 291**
- Российских ОС: **9**
- Российского ПО: **65**

Операционные системы

Вендоры ПО

А что с данными? Российский IT-сегмент

Государственный источник

БДУ ФСТЭК

- Дата создания: март 2015
- Уязвимостей: **44 836**
- Вендоров ПО: **1 291**
- Российских ОС: **9**
- Российского ПО: **65**

Операционные системы

ASTRA LINUX®

РЕДОС

alt linux
ALT LINUX TEAM

ROSA

ОСНОВА

АВРОРА

СТРЕЛЕЦ
ОПЕРАЦИОННАЯ СИСТЕМА ОБЩЕГО НАЗНАЧЕНИЯ

ФССП России
GosLinux

UB Linux

Вендоры ПО

KASPERSKY lab

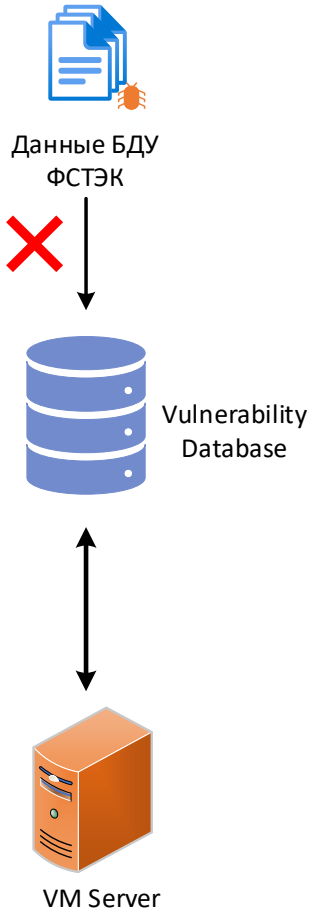
WEBSOFT

РУБИНТЕХ
технологии информационной безопасности

РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

16 201	5 485
Включено ПО в Реестр	Правообладателей

Одной БДУ ФСТЭК не достаточно



фродекс

К чему стремиться

✓ Разработчикам российского ПО:

- **Публиковать данные об уязвимостях**
- **Публиковать обновления безопасности**
- **Придерживаться общепринятых стандартов описания уязвимостей**

✓ Регулятору:

- **Ввести общепринятый стандарт описания уязвимостей, при необходимости дополнить его**
- **Обязать разработчиков отечественного ПО публиковать данные об уязвимостях, и делать это в соответствии со стандартом**
- **Развивать программы «Bug Bounty», оказывать содействие компаниям-разработчикам в организации данных программ**

фродекс

Андрей Никонов

Старший инженер-программист


a.nikonov@frodex.ru


+7(495) 967 65 19


frodex.ru


Техническая поддержка:
support@frodex.ru


офис
г.Уфа, ул. Пархоменко, 133/1, 2 этаж