

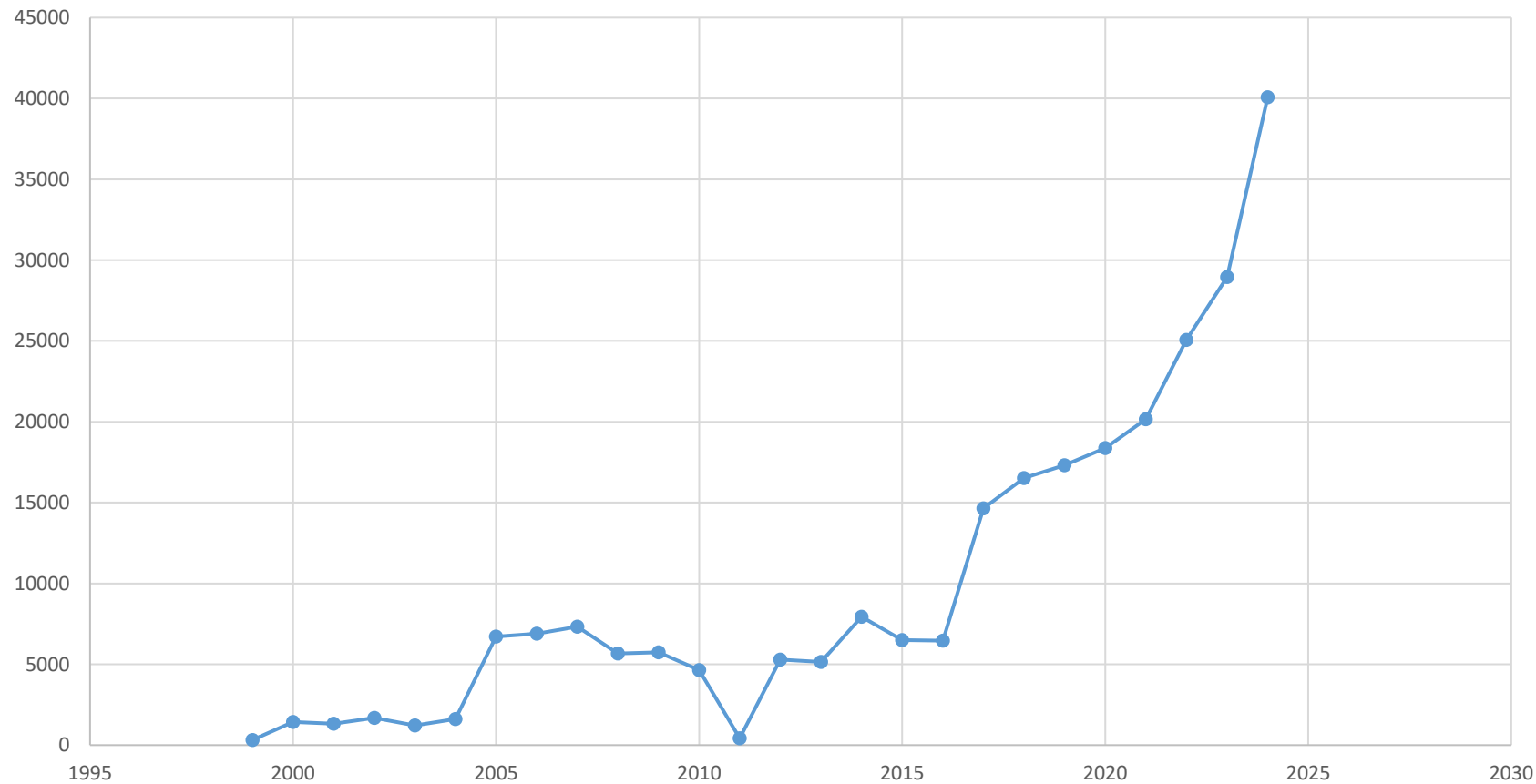
# **Исследование защищенности с помощью Сканер-ВС 7**

**Ким Алина, специалист центра кибербезопасности ГК «Эшелон»**

# План

1. Актуальность
2. Подходы к поиску уязвимостей
3. Сканер-ВС 7

# Количество опубликованных CVE



2024	40 077
2023	28 961
2022	25 059
2021	20 161
2020	18 375
2019	17 308
2018	16 512
2017	14 645
2016	6 457
2015	6 494
2014	7 948
2013	5 142
2012	5 288
2011	415
2010	4 639
2009	5 732
2008	5 673
2007	7 322
2006	6 885
2005	6 708
2004	1 612
2003	1 223
2002	1 691
2001	1 323
2000	1 438
1999	321

<https://www.cve.org/about/Metrics>

2025

**38 791**  
опубликованных  
CVE

**135**  
уязвимости  
в день

## NVD Dashboard

### CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	325	127	0	2
This Week	418	127	0	2
This Month	2037	1859	0	46
Last Month	4536	3797	0	319
This Year	38791	32616	0	2688

# Путь уязвимости

307 000 (NIST NVD)

1. Уязвимость  
обнаружена

3. Эксплойт  
нулевого дня

5. Исправление

7. Эксплойт

2. Назначен  
идентификатор

4. Появилась  
информация  
о готовящемся  
исправлении

6. Опубликован  
бюллетень

8. Включена  
в KEV

~1 300 (KEV –  
Known  
Exploitable  
Vulnerabilities)

Уязвимость  
нулевого дня

Half-day  
vulnerability

Известная  
уязвимость

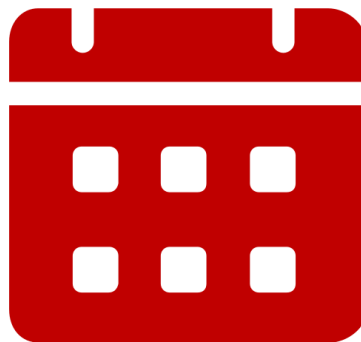
# Причины возникновения уязвимостей



Ошибка в коде



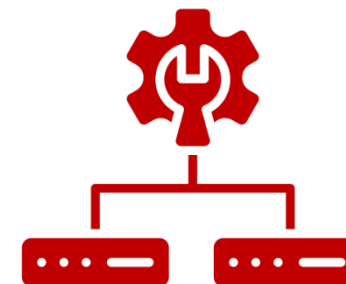
Слабые меры  
безопасности



Устаревшее ПО



Человеческий  
фактор



ИТ  
инфраструктура

# Цикл управления уязвимостями



**Самое важное –  
иметь надежный,  
простой и гибкий  
в использовании  
инструмент для  
выявления  
уязвимостей.**

# Технологии поиска уязвимостей

Поиск уязвимостей  
по версиям

Разработка скриптов для  
каждой уязвимости

XML-описания для  
каждой уязвимости  
(OVAL)





# Скрипты

```
# Описание скрипта
if (description) {
    script_name("Пример NASL: Проверка порта 80");
    script_description("Проверяет, открыт ли порт 80 на
целевой машине.");
    script_summary("Отправляет HTTP-запрос и анализирует
ответ.");
    script_category(ACT_GATHER_INFO);
    script_family("Сетевые проверки");
    exit(0);
}
```

```
# Проверка открытого порта
port = 80;
if (!get_port_state(port)) {
    exit(0); # Порт закрыт
}
```

Nessus Attack Scripting Language

## Проблемы данного подхода:

- Нужно поддерживать несколько десятков тысяч плагинов/скриптов, выявляющих уязвимости
- Сканирование одного узла может занимать десятки минут
- Возможность добавлять собственные скрипты ограничена или полностью отсутствует



# XML

```
<metadata>
  <title>Microsoft SQL Server 2017 is installed</title>
  <affected family="windows">
    <platform>Microsoft Windows 8.1</platform>
    <platform>Microsoft Windows 10</platform>
    <platform>Microsoft Windows Server 2012 R2</platform>
    <platform>Microsoft Windows Server 2016</platform>
    <product>Microsoft SQL Server 2017</product>
  </affected>
  <reference source="CPE" ref_id="cpe:/a:microsoft:sql_server:2017" />
  <description>Microsoft SQL Server 2017 is installed</description>
</metadata>
<criteria>
  <criterion comment="Check if HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\.*\Setup!SQLPath exists" test_ref="oval:ru.altx-soft.win:tst:75762" />
  <criterion comment="Check if SQL Server instances with version greater
than or equal 2016.140.500.272 and less than 2018.150.0.0 exist"
test_ref="oval:ru.altx-soft.win:tst:50755" />
</criteria>
</definition>
```

## Проблемы данного подхода:

- Нужны агенты для проверки систем
- Сложно создавать собственные правила



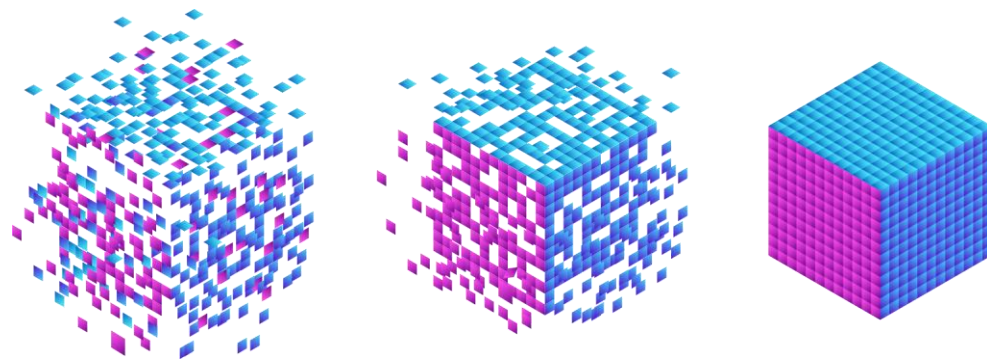
# Использование агрегированной базы данных уязвимостей

Российские источники:

- БДУ ФСТЭК России
- Базы Astra Linux, Ред ОС

Иностранные источники:

- NIST National Vulnerability Database
- База обновлений Windows
- RHEL/CentOS Security Data
- Ubuntu CVE Tracker
- Debian GNU/Linux Security Bug Tracker
- ...



# База уязвимостей Сканер-ВС онлайн



<https://vulnerabilities.etecs.ru/>

**Поиск и сортировка**  
Показать поиск и сортировку

**Поиск**  
Поиск по ИД или описанию...

**Сортировать по**  
Сортировать по: Оценка EPSS  
Порядок сортировки: По убыванию

**Фильтры по оценкам**  
Диапазон CVSS: МИН, МАКС (Range: 0.0 - 10.0)  
Диапазон EPSS: МИН, МАКС (Range: 0.000 - 1.000)

**Sources**  
ancho\_re\_overrides, astra, bdu, debian, msrc, nvd, redhat, redos, ubuntu

**СПАСИБО ЗА ВНИМАНИЕ!**