****

**Содержание**

[**Введение 2**](#_heading=h.gjdgxs)

[**I. Задание**](#_heading=h.2592qc799d1r) **3**

[**II. Ход работы: 4**](#_heading=h.v6umh3ovq62o)

[**Вывод по работе. 8**](#_heading=h.t0p55bvsw0th)

[**Список использованных источников 9**](#_heading=h.n1751prodfc8)

# Введение

Цель работы – получить знания и навыки работы с различными базами данных угроз и уязвимостей. Работа индивидуальная.

Для достижения поставленной цели необходимо решить следующие задачи:

* 1; Обязательный материал для ознакомления:
* 2; БД угроз и уязвимостей (описываем 5 БД и прикладываем пару скриншотов):
* 3. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)

**Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей**

## Задание

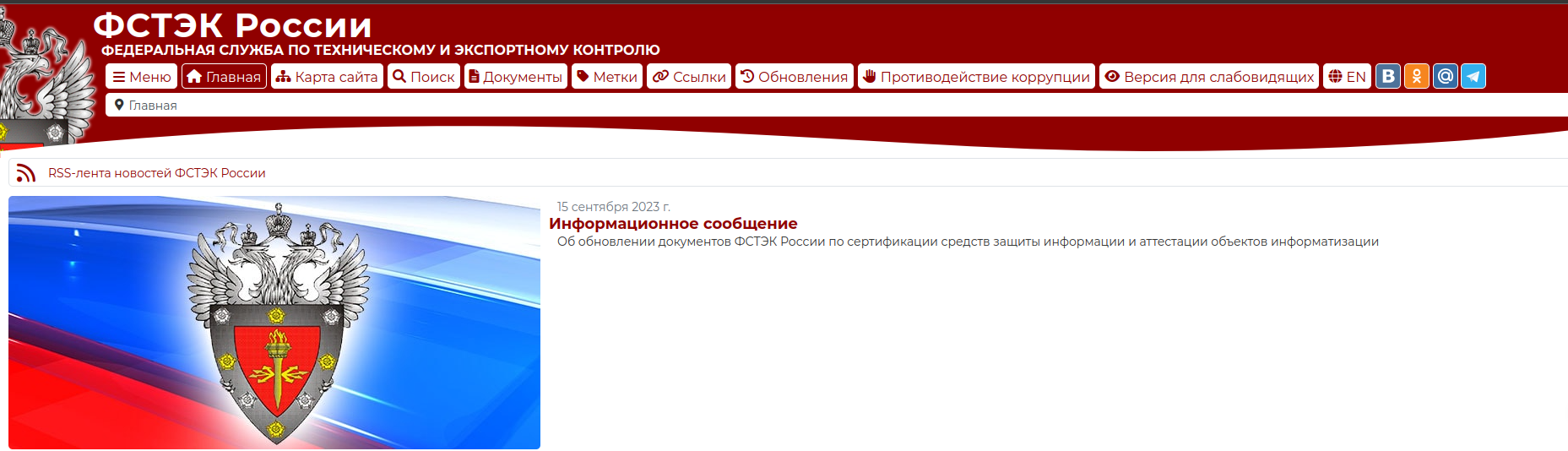
1. Обязательный материал для ознакомления:
   1. <https://habr.com/ru/company/pt/blog/266485/>
   2. <https://habr.com/ru/company/ic-dv/blog/453756/>
   3. [https://xakep.ru/2009/05/15/48221/#toc01.](https://xakep.ru/2009/05/15/48221/#toc01)
   4. <https://habr.com/ru/company/xakep/blog/305262/>
2. БД угроз и уязвимостей (описываем 5 БД и прикладываем пару скриншотов):
   1. ФСТЭК
   2. Vulners
   3. CVE (NVD)
   4. cert/cc
   5. secunia
   6. exploit in
   7. X-Force
   8. SecurityFocus
   9. CNNVD
   10. JVN
   11. https://www.exploit-db.com

1. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)

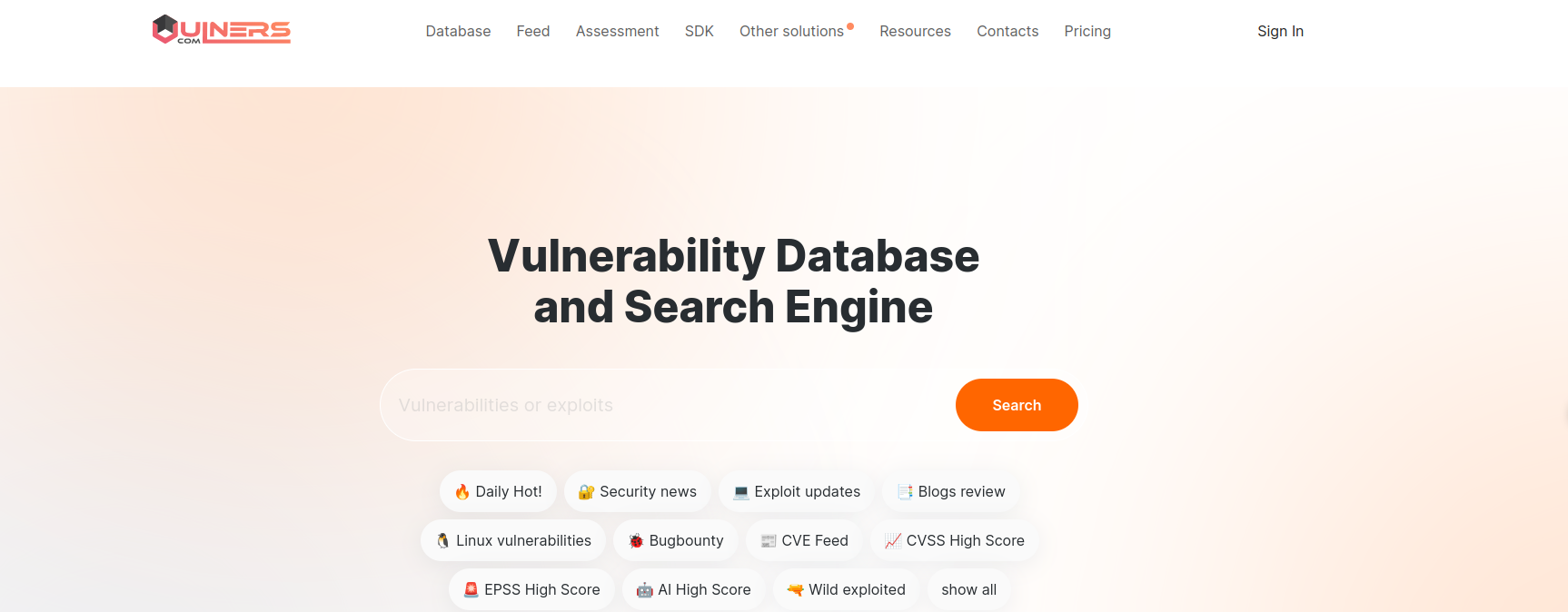
## II. Ход работы:

* 1. ФСТЭК

ФСТЭК России - это Федеральная служба по техническому и экспортному контролю. Это федеральный орган исполнительной власти, который отвечает за обеспечение безопасности информационных технологий и систем в Российской Федерации.

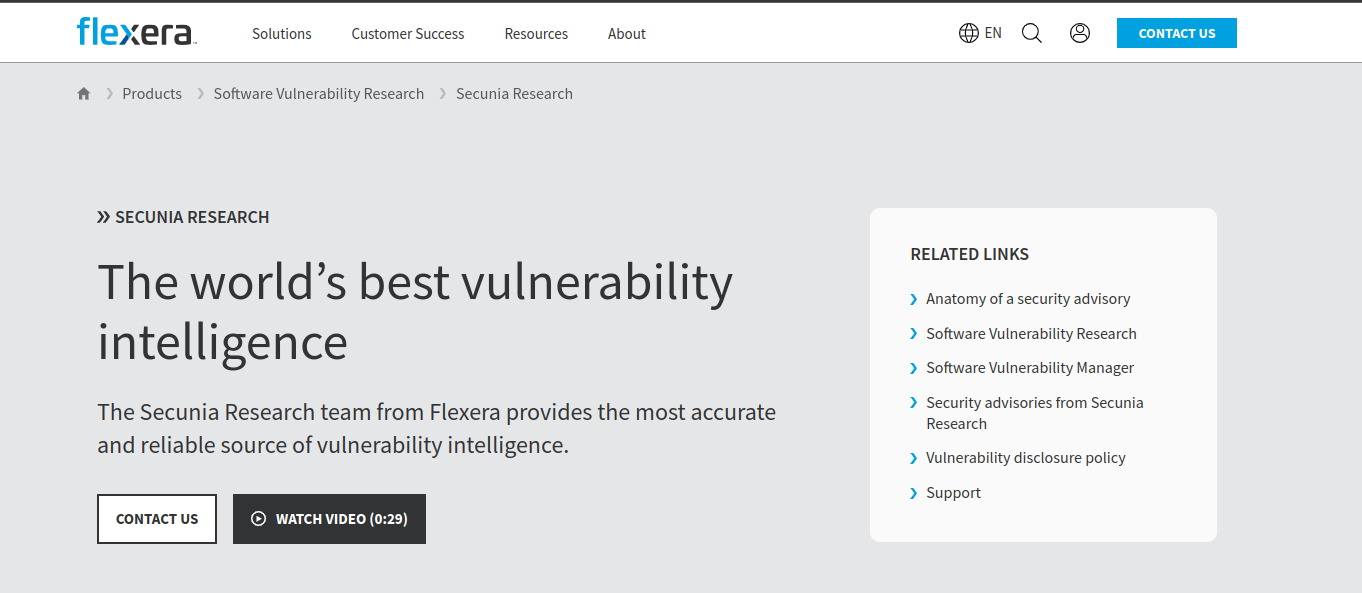
2. Vulners

Vulners - это база данных и сканер уязвимостей, который предоставляет информацию о безопасности программного обеспечения и систем. Vulners собирает информацию из более чем 200 источников, включая CVE, NVD, BugTraq и другие. Эта информация включает в себя описание уязвимости, ее критичность, доступные эксплоиты и патчи.



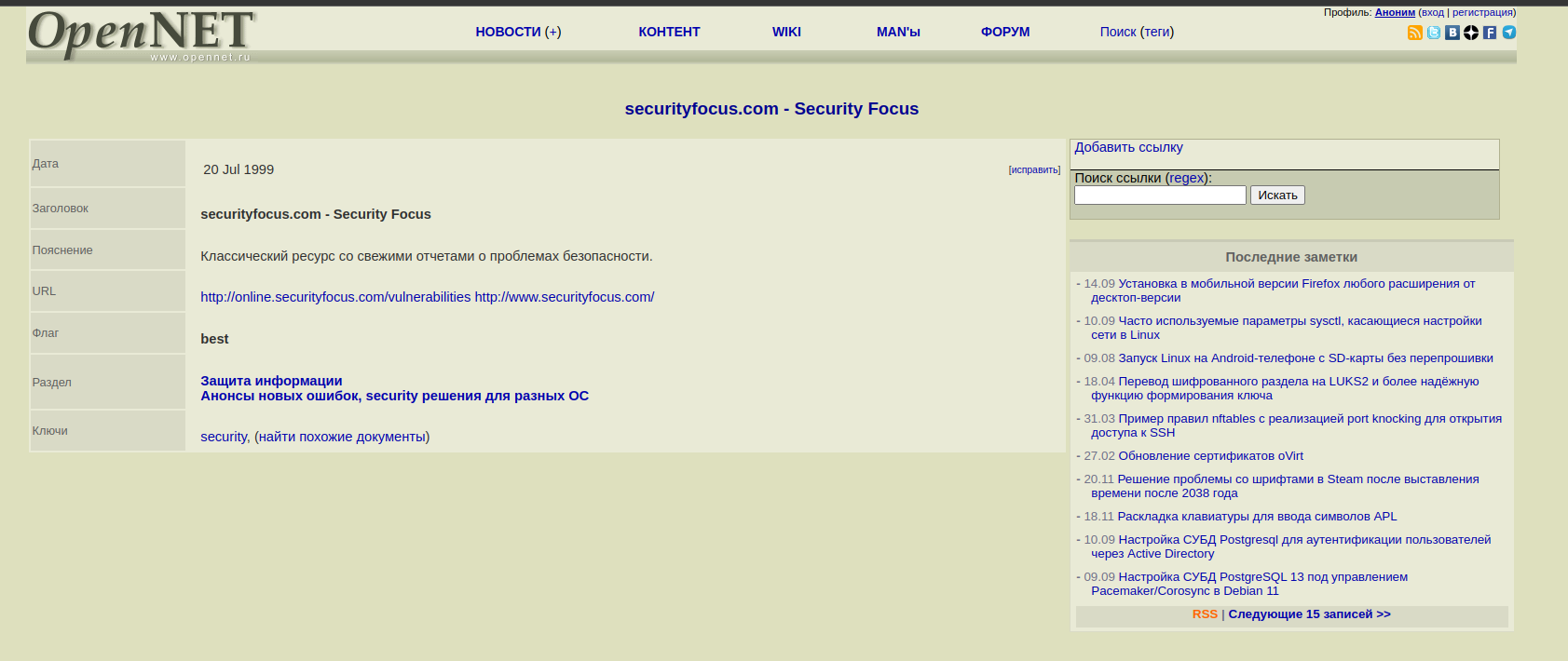
3. Secunia

Secunia - это компания, которая занимается разработкой программного обеспечения для обеспечения безопасности. Она была основана в 2001 году в Швеции и имеет офисы в Швеции, США и Великобритании. Secunia предлагает широкий спектр продуктов и услуг.



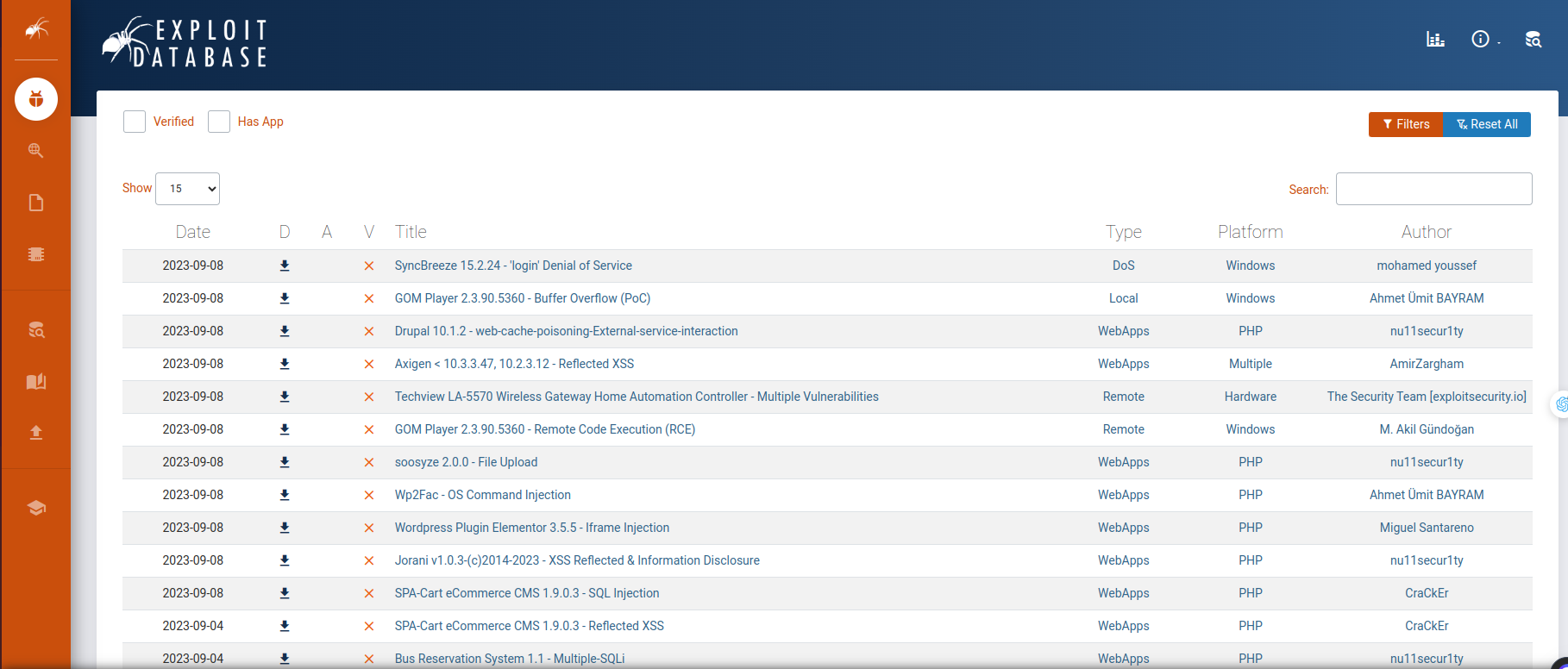
4. SecurityFocus

SecurityFocus - это новостной онлайн-портал компьютерной безопасности и поставщик услуг информационной безопасности. Он был основан в 1999 году и в настоящее время принадлежит компании Tenable Network Security.



5. <https://www.exploit-db.com>

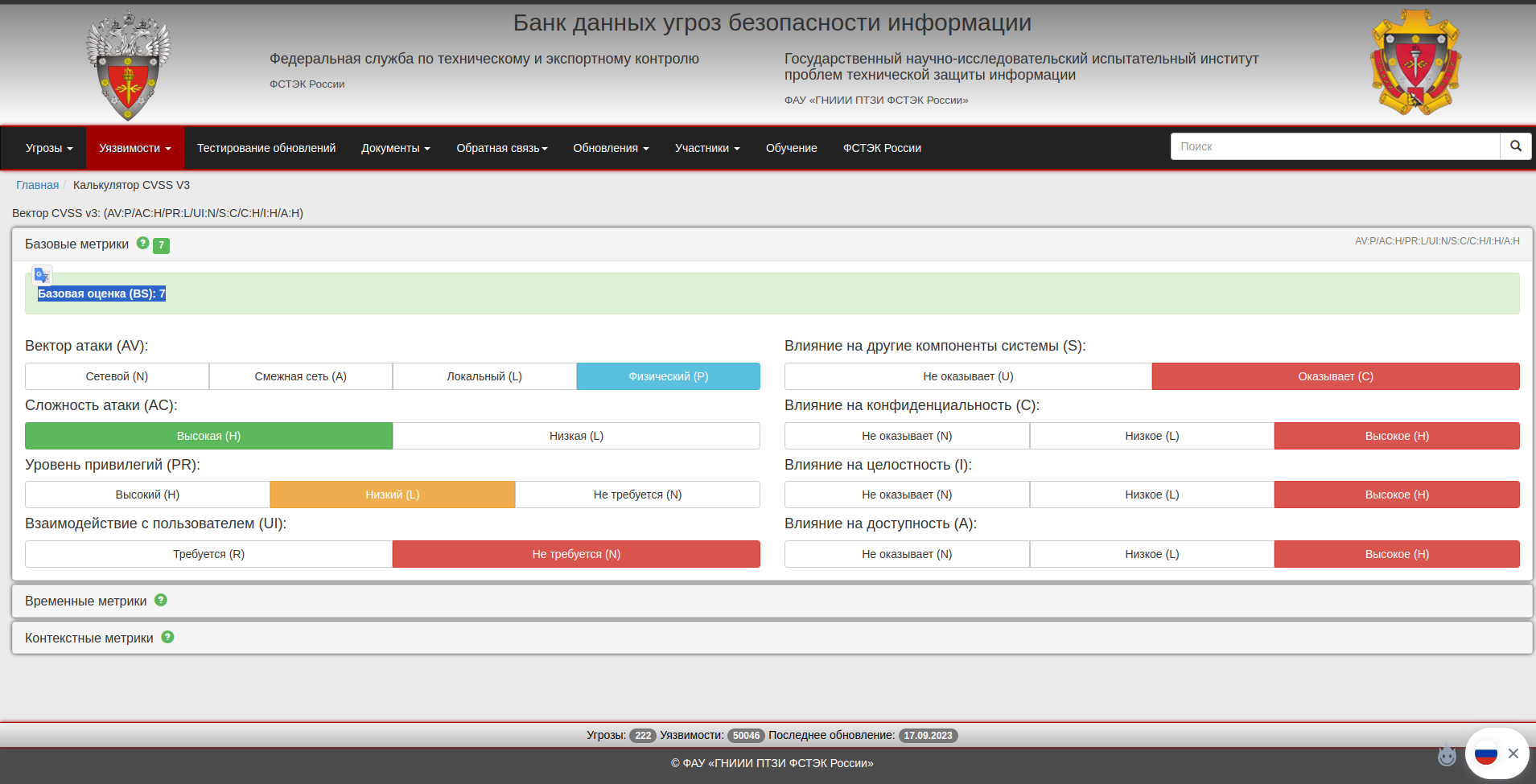
Exploit Database - это архив публичных эксплойтов и соответствующего уязвимого программного обеспечения, который создается и поддерживается для тестировщиков на проникновение и исследователей уязвимостей.



**3. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)**

**3.1 Оцените уязвимости по базовым метрикам для ситуации при следующих условиях:**

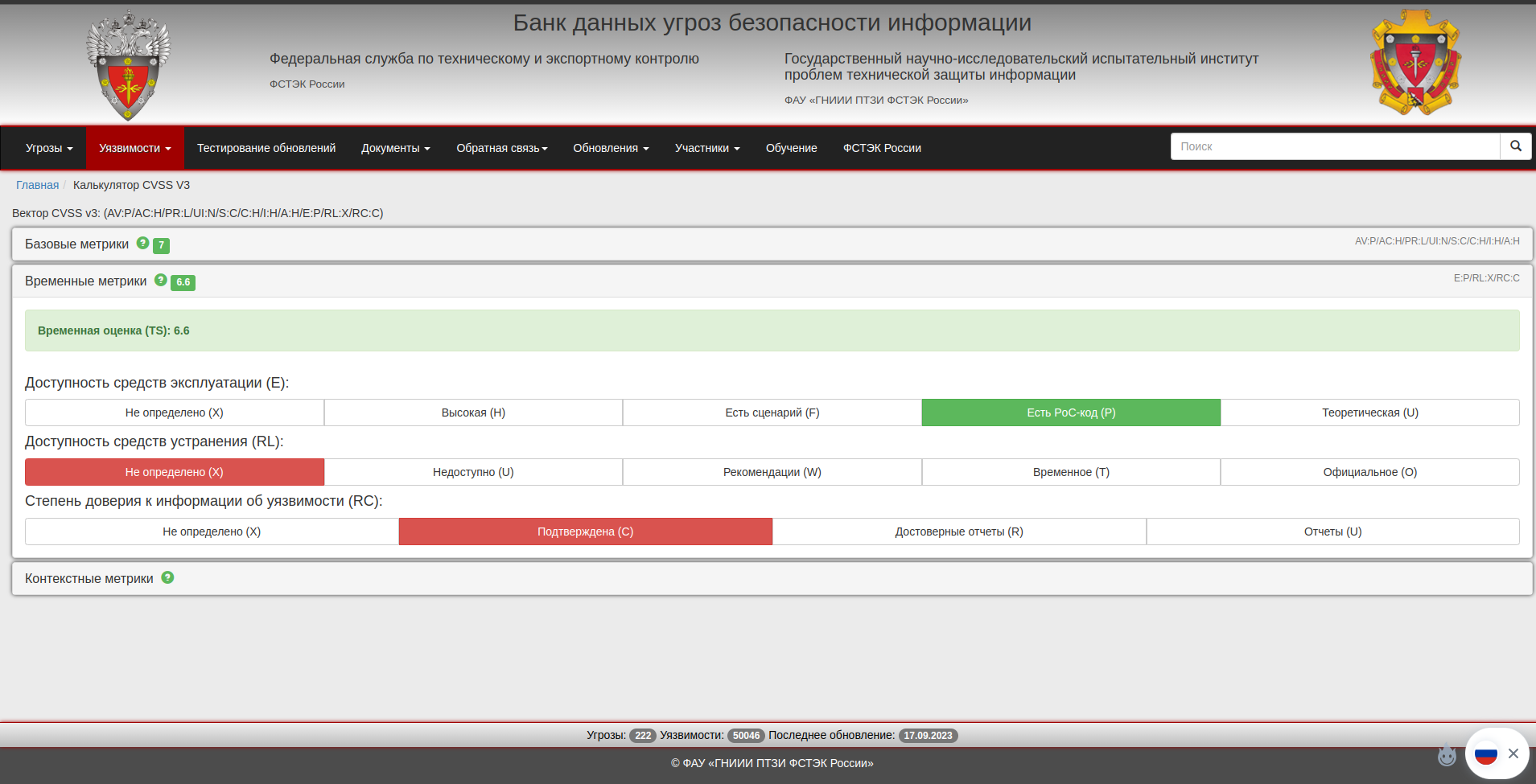
в) атака высокой сложности будет проводится на физический уровень системы, при этом оказывается влияние на другие компоненты системы. Однако атака приводит только к нарушению всех свойств ИБ низкого уровня. Взаимодействие с пользователем не требуется, а уровень привилегий - низкий.



AV:P/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H Базовая оценка (BS): 7

**3.2** **Оцените уязвимости по временным метрикам для ситуации при следующих условиях:**

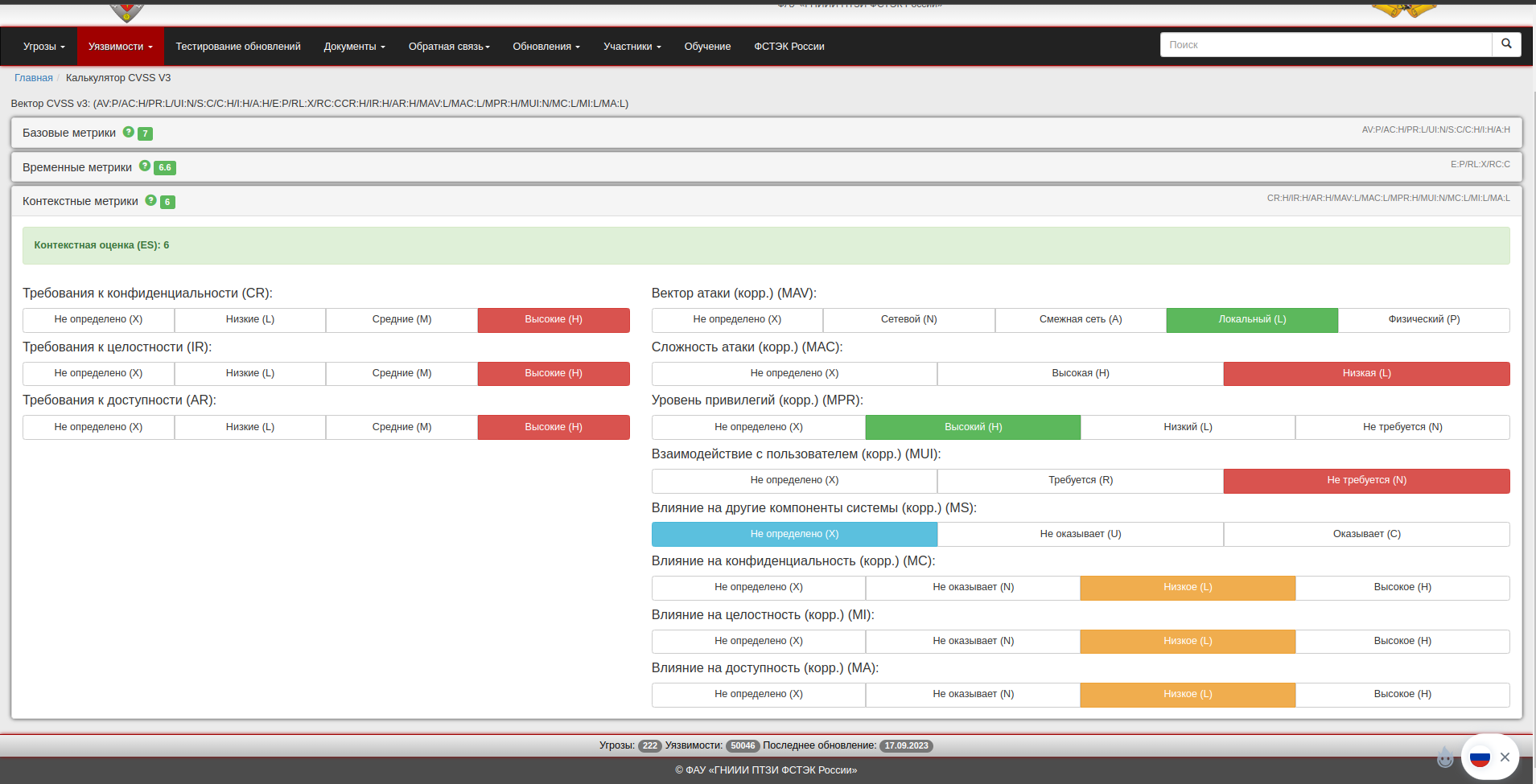
в) Предполагается, что есть PoC-код для средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.



E:P/RL:X/RC:C Временная оценка (TS): 6.6

**3.3 Оцените уязвимости по контекстным метрикам для ситуации при следующих условиях:**

в) К уровню обеспечения КЦД заданы высокие требования, влияние на них также оказывается высоким. При этом проводится атака низкой сложности на локальный уровень системы. Уровень привилегий в данном случае - высокий, взаимодействия с пользователем не происходит. Оказывается ли влияние на другие компоненты системы - неизвестно.



CR:H/IR:H/AR:H/MAV:L/MAC:L/MPR:H/MUI:N/MC:L/MI:L/MA:L Контекстная оценка (ES): 6

# Вывод по работе.

1. Идентификация угроз и уязвимостей

Первый шаг к обеспечению безопасности базы данных - это выявление возможных угроз и уязвимостей. Это можно сделать с помощью следующих методов:

* Анализ доступа к данным
* Настройка прав доступа
* Проверка обновлений и заплаток
* Другие меры безопасности

2. Классификация и оценка рисков

После идентификации угроз и уязвимостей необходимо оценить потенциальные риски, связанные с каждой из них. Это можно сделать с помощью следующих методов:

* Использование калькулятора уязвимостей
* Другие методы оценки рисков

3. Разработка мер безопасности

На основе исследования баз данных угроз и уязвимостей необходимо разработать план мер безопасности, который включает в себя следующие рекомендации:

* Устранение или снижение уязвимостей
* Улучшение процедур доступа и аутентификации
* Регулярные проверки безопасности
* Обновления системы

4. Обучение и осведомленность

Обучение персонала и повышение осведомленности о безопасности данных являются важными частями эффективной защиты баз данных. Это включает в себя:

* Регулярные тренинги
* Информирование сотрудников о правилах безопасности
* Соблюдение политик информационной безопасности

5. Мониторинг и обновление

Регулярный мониторинг баз данных и обновление мер безопасности позволяют быстро реагировать на новые угрозы и уязвимости. Это включает в себя:

* Проверку наличия обновлений программного обеспечения
* Применение исправлений безопасности
* Мониторинг журналов активности

# Список использованных источников

<https://bdu.fstec.ru/calc3>

<https://www.exploit-db.com>

<https://www.opennet.ru/links/info/428.shtml>

<https://www.flexera.com/products/software-vulnerability-research/secunia-research>

<https://vulners.com/search?query=https://fstec.ru/>

<https://fstec.ru/>