ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет безопасности информационных технологий

Дисциплина:
«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1
Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей

Выполнил:
Студент гр. N3253
Пастухова А.А.

Проверил:
Якимова С.А.

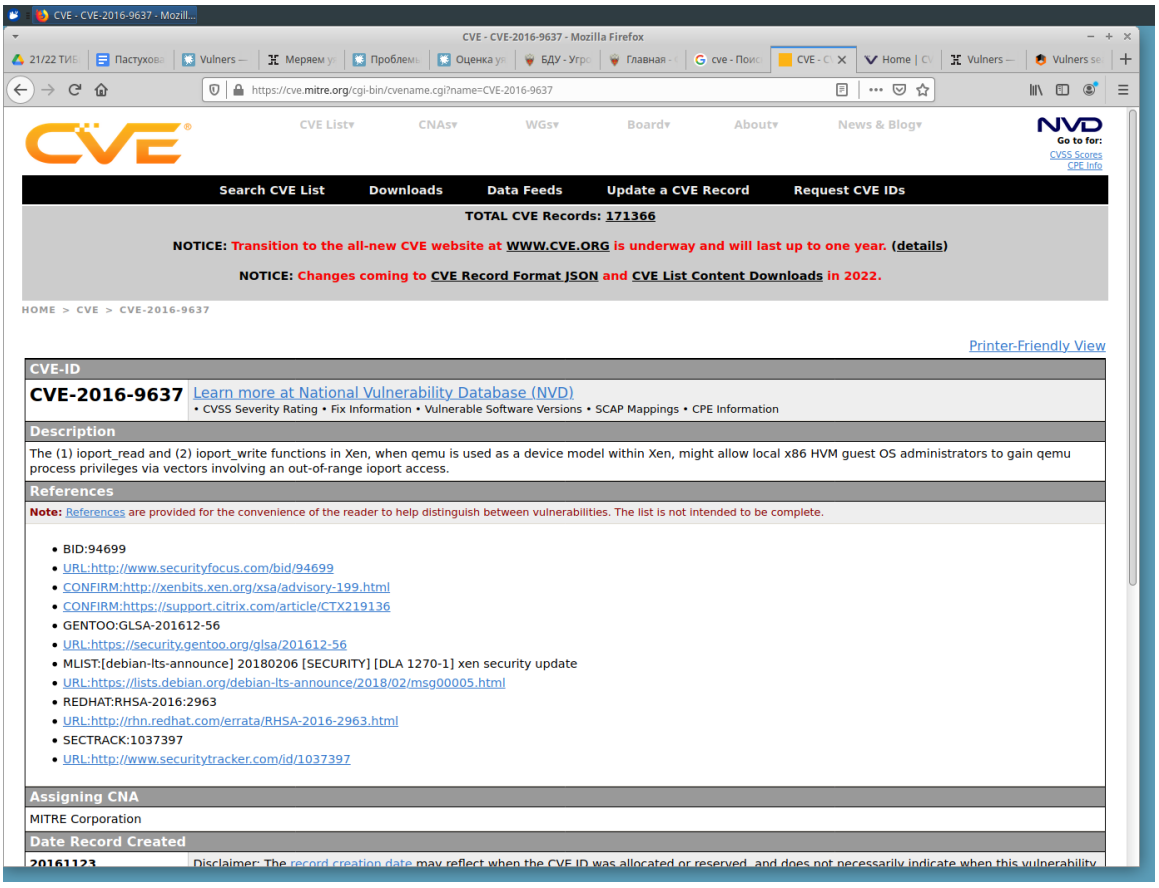
Санкт-Петербург
2022г.

Цель работы: получить знания и навыки работы с различными базами данных угроз и уязвимостей.

Ход работы:

1. CVE (Common Vulnerabilities and Exposures)

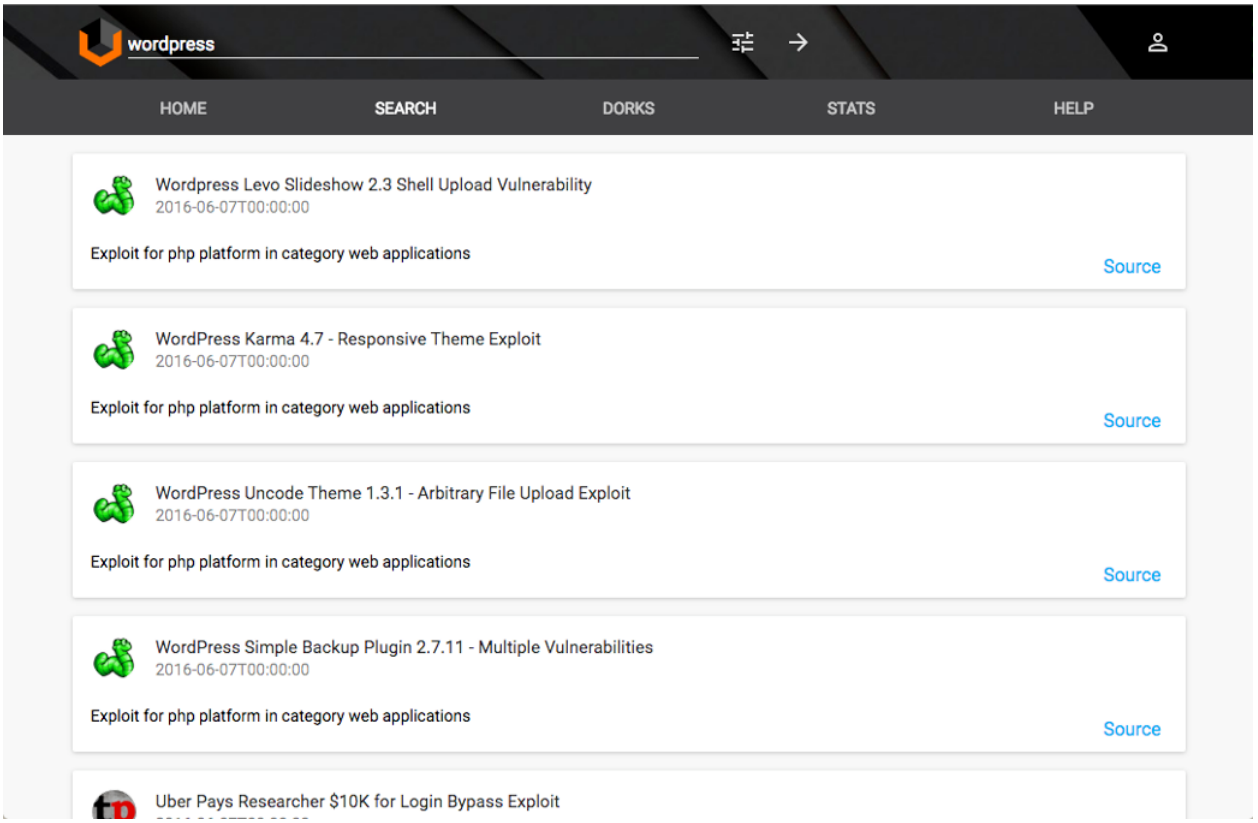
Так называемый "словарь" известных уязвимостей, имеющий строгую характеристику по описательным критериям. Полностью CVE можно отыскать в Национальной Базе Уязвимостей США (National Vulnerability Database). Общий вид записи CVE выглядит примерно так: CVE ID, Reference и Description, ID записывается с указанием кода и порядкового номера. В поле Reference записываются различного рода ссылки на патчи, рекомендательного рода документы или комментарии разработчика. Description отвечает за описание самой уязвимости.



2. Vulners

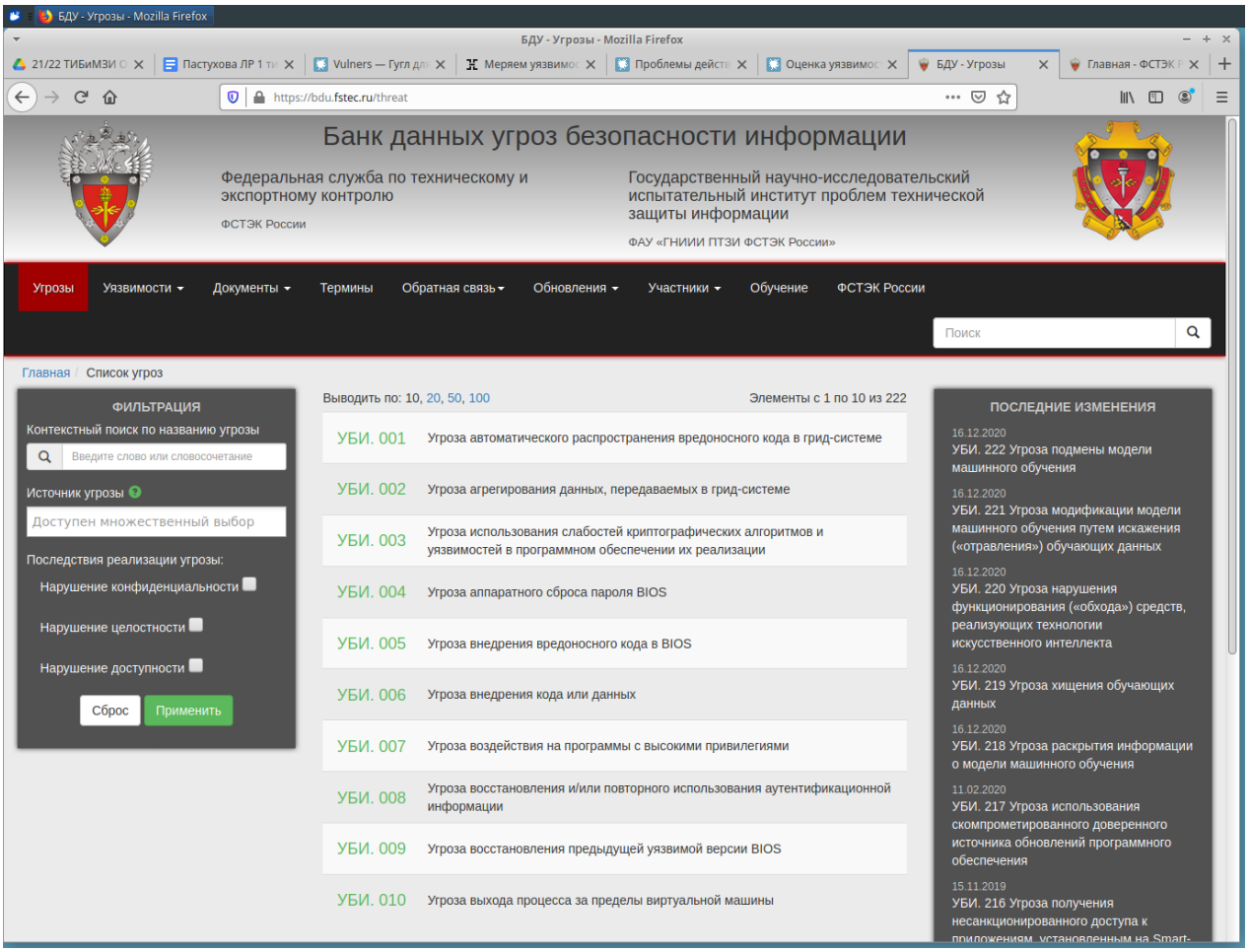
Очень большая и непрерывно обновляемая база данных ИБ-контента. Он агрегирует и представляет в удобном виде шесть основных типов данных: популярные базы уязвимостей, вендорские бюллетени безопасности, эксплоиты из Exploit-DB и Metasploit, Nessus-плагины для детекта

уязвимостей, дисклозы багов с сайтов bug bounty программ, публикации на тематических ресурсах.



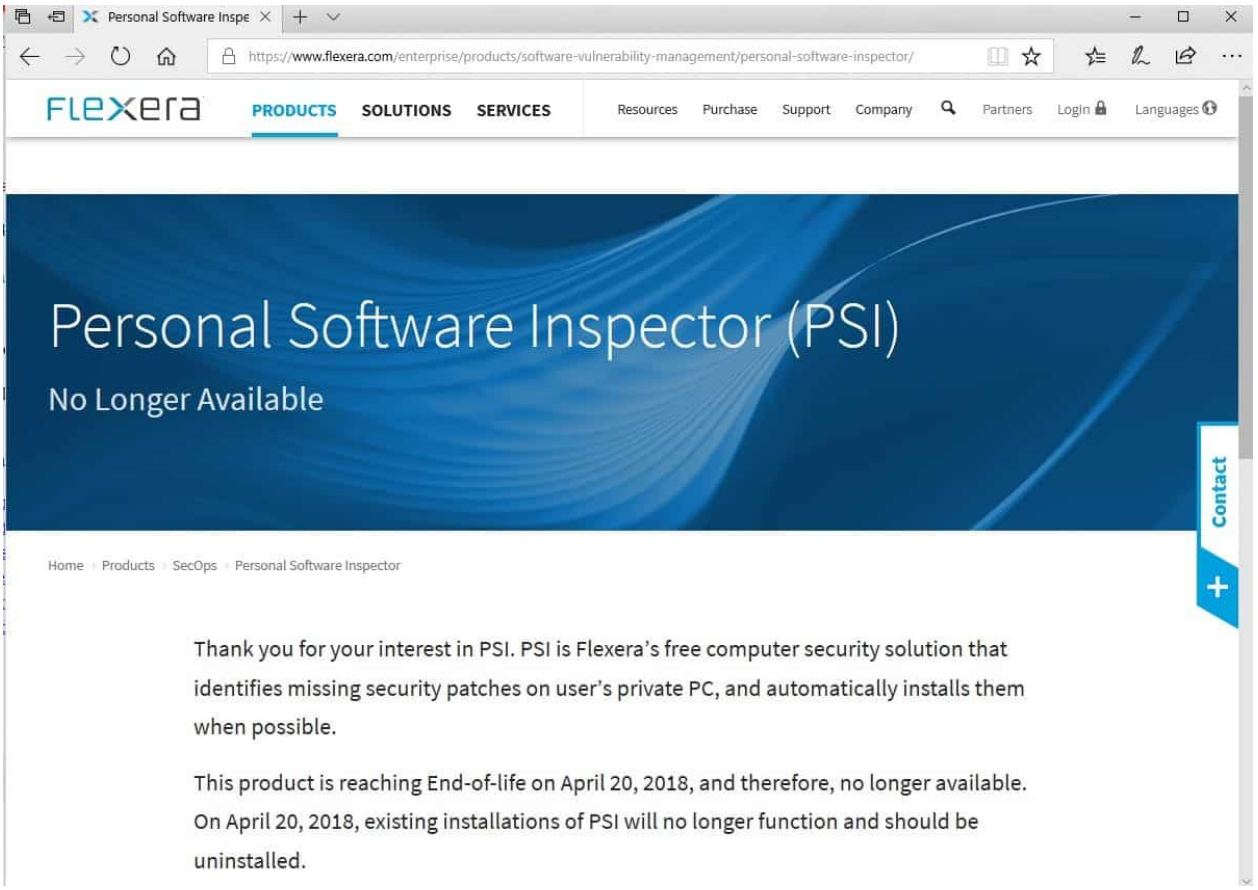
3. ФСТЭК

Федеральная служба по техническому и экспортному контролю. База данных содержит перечень угроз и уязвимостей программного обеспечения, согласно законодательству РФ. Список постоянно пополняется и обновляется.



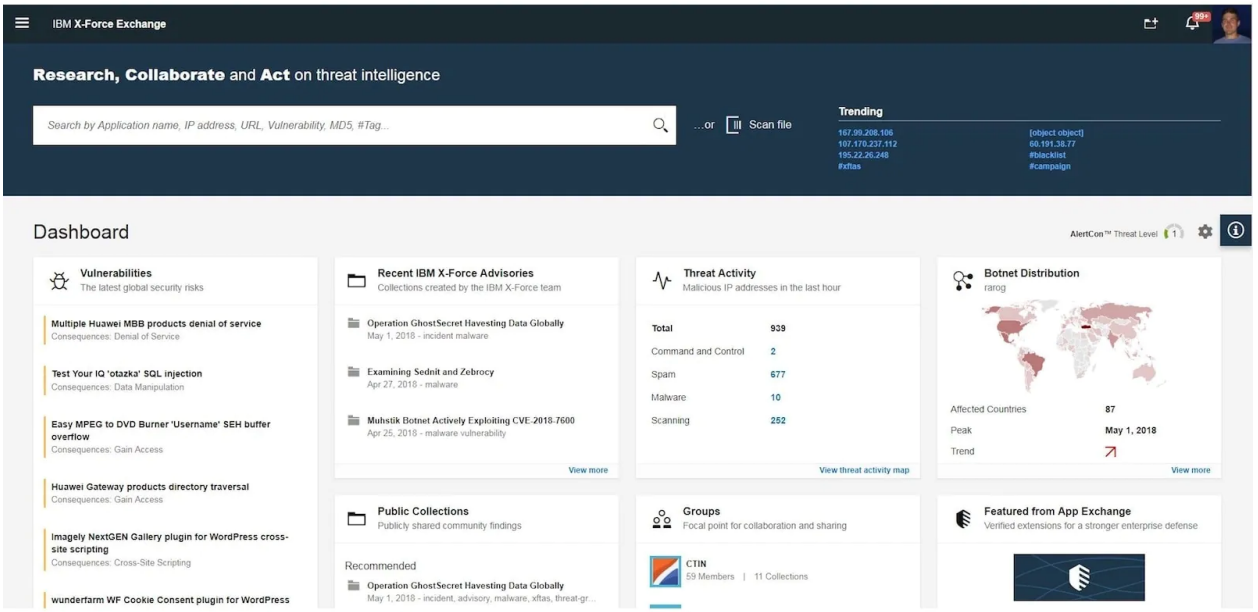
4. Secunia

Датская компания, специализирующаяся на компьютерной и сетевой безопасности. Наиболее известна своими тестами на наличие уязвимостей, которые прошли более 12,400 программных продуктов и операционных систем. Подписка платная.



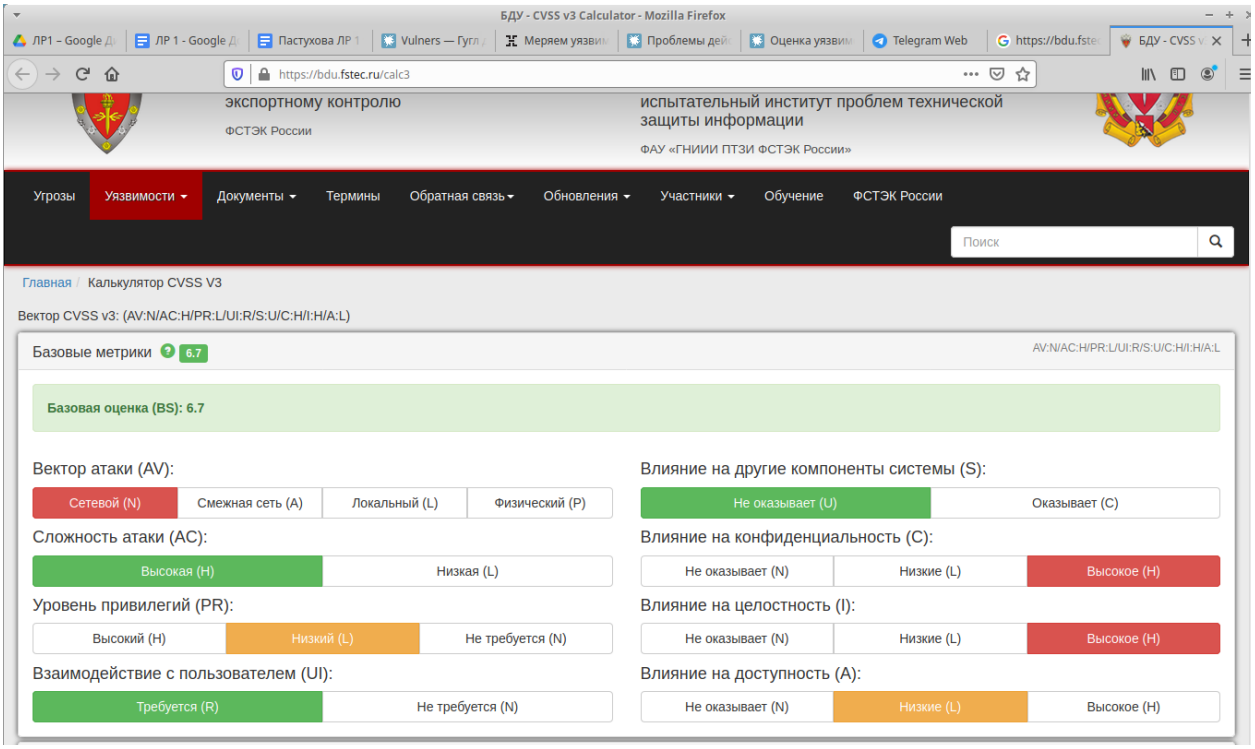
5. X-Force

Облачная платформа для обмена аналитическими данными об угрозах, которая позволяет быстро исследовать новейшие угрозы безопасности, собирать практически полезные аналитические данные и сотрудничать с коллегами. Кроме всего прочего также описывает материальный ущерб, который может повлечь за собой угроза эксплуатации.



1. Оцените уязвимость по базовым метрикам для ситуации при следующих условиях:

е) атака высокой сложности будет проводится на сетевой уровень системы, при этом не оказывается влияние на другие компоненты системы. Атака приводит к нарушению конфиденциальности и целостности высокого уровня, доступности низкого уровня. При этом требуется взаимодействие с пользователем, уровень привилегий - низкий.

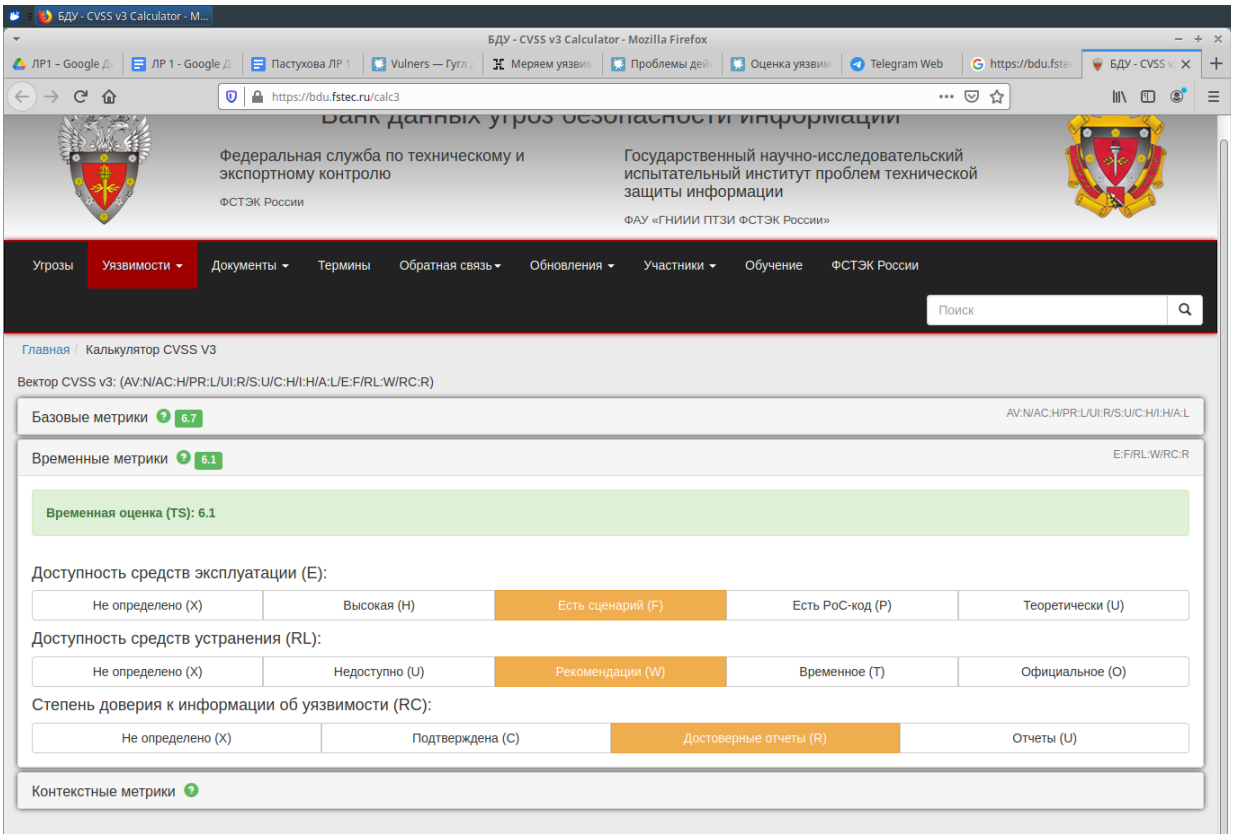


Результат 6.7

2. Оцените уязвимость по временным метрикам для ситуации при следующих условиях:

е) Предполагается, что есть сценарий для средств эксплуатации, есть рекомендации для средств устранения, а информация об уязвимостях получена из достоверных отчетов.

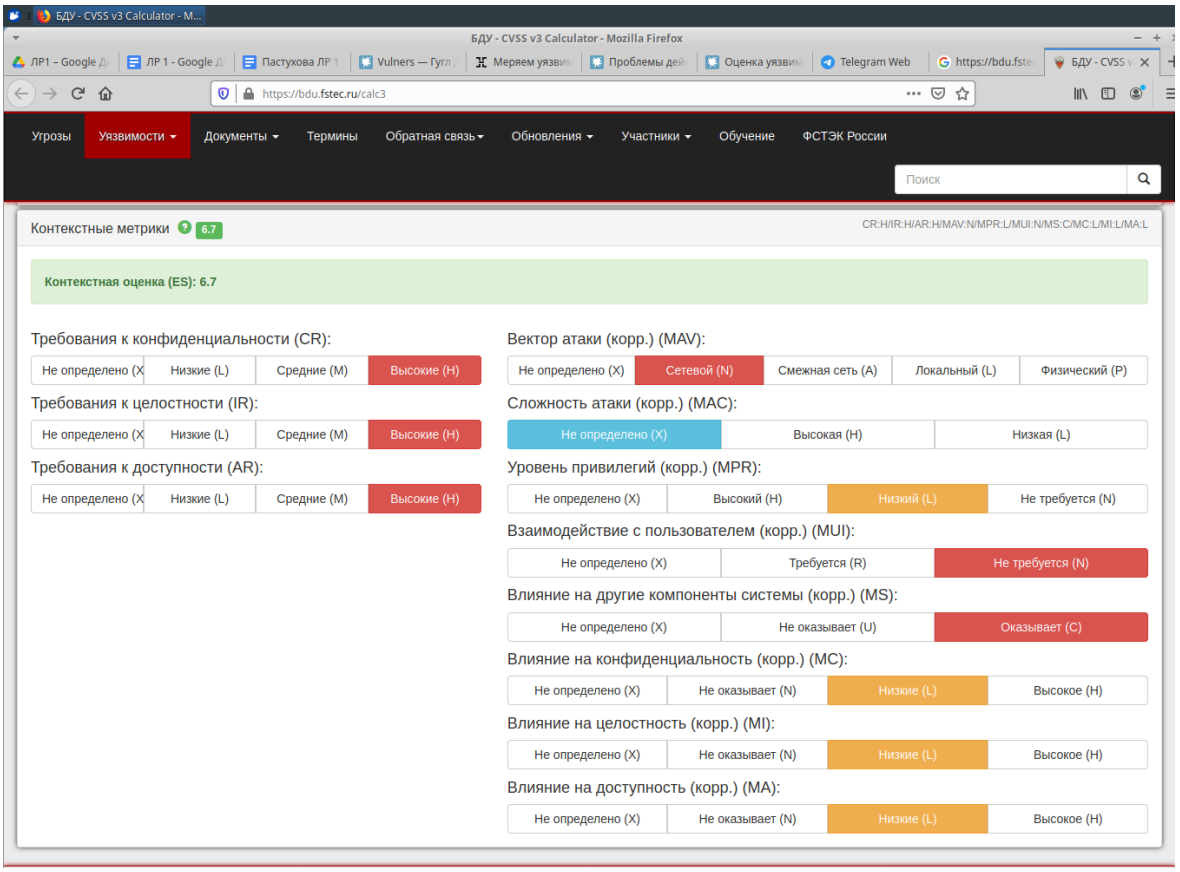
Результат 6.1



3. Оцените уязвимости по контекстным метрикам для ситуации при следующих условиях:

е) К уровню обеспечения КЦД заданы высокие требования, однако влияние оказывается низким. При этом проводится атака неопределенной сложности на сетевой уровень системы. Уровень привилегий в данном случае - низкий, взаимодействия с пользователем не происходит. Также оказывается влияние на другие компоненты системы.

Результат 6.7



Вывод: я получила знания и навыки работы с различными базами данных угроз и уязвимостей. Также изучила материалы касательно метрик и калькулятора CVSS v3, посчитала базовые, временные и контекстные метрики для гипотетической ситуации.