ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет информатики и вычислительной техники

Дисциплина:
«*Теория информационной безопасности и методология защиты информации*»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

Выполнил:
Студент гр. P3231
Кислицин Алексей Андреевич

Проверил:
Есипов Дмитрий Андреевич,
инженер ФБИТ

Санкт-Петербург
2022г.

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

Объекты:

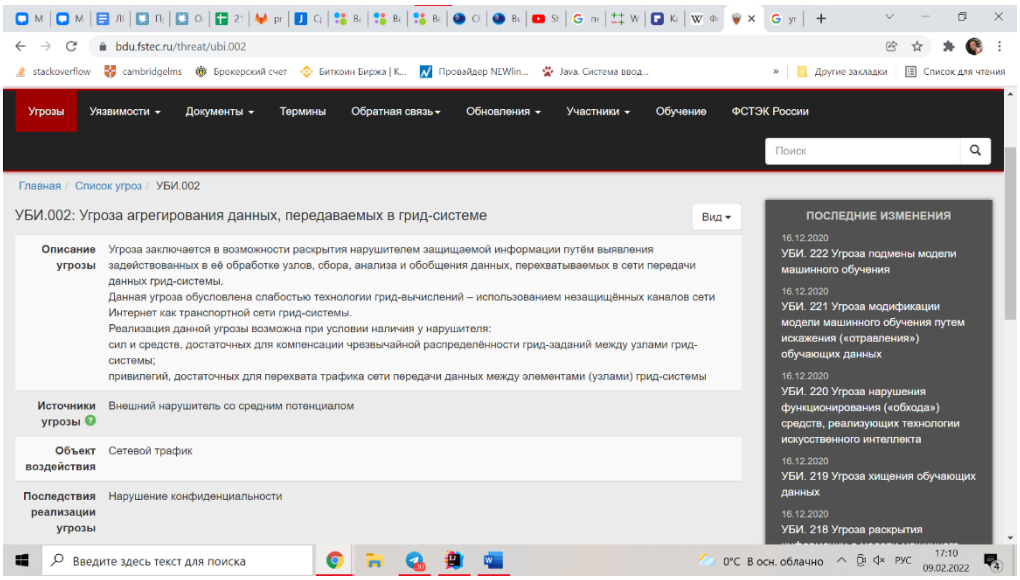
1. Обязательный материал для ознакомления:
   - 1.1 https://habr.com/ru/company/pt/blog/266485/
   - 1.2 https://habr.com/ru/company/ic-dv/blog/453756/
   - 1.3 https://xakep.ru/2009/05/15/48221/#toc01.
   - 1.4 https://habr.com/ru/company/xakep/blog/305262/
2. БД угроз и уязвимостей:
   - 2.1 ФСТЭК
   - 2.2 Vulners
   - 2.3 CVE (NVD)
   - 2.4 cert/cc
   - 2.5 secunia
   - 2.6 exploit in
   - 2.7 X-Force
   - 2.8 SecurityFocus
   - 2.9 CNNVD
   - 2.10 JVN
   - 2.11 https://www.exploit-db.com
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)

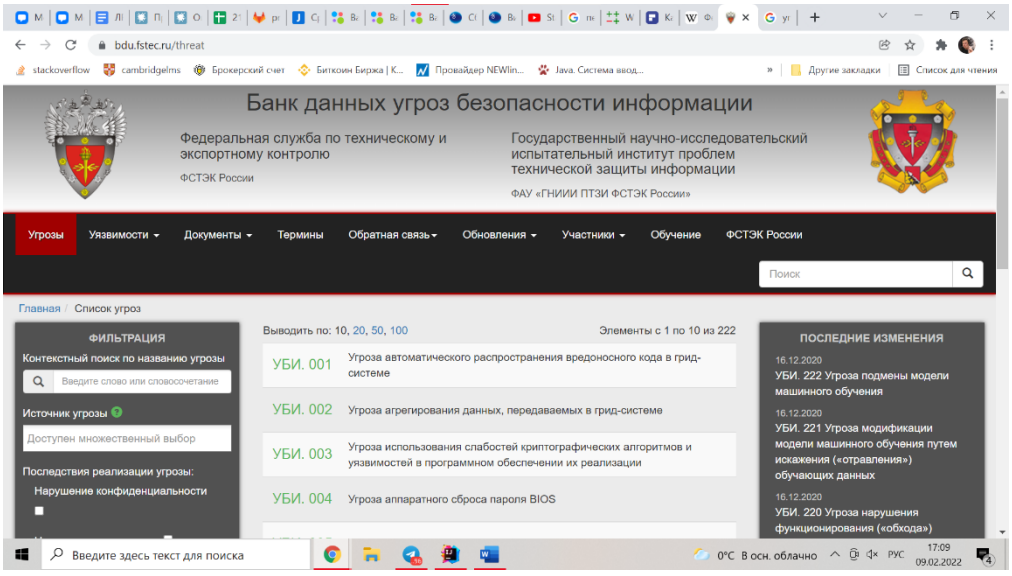
Ход работы:

1. **ФСТЭК**

ФСТЭК – это федеральная служба по техническому и экспортному контролю.

ФСТЭК утвердили «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» 14 февраля 2008 года. Эта методика является единственным утвержденным документом по определению актуальных угроз безопасности. База данных уязвимостей ФСТЭК является крупнейшей базой уязвимостей на русском языке.





2. **Vulners**

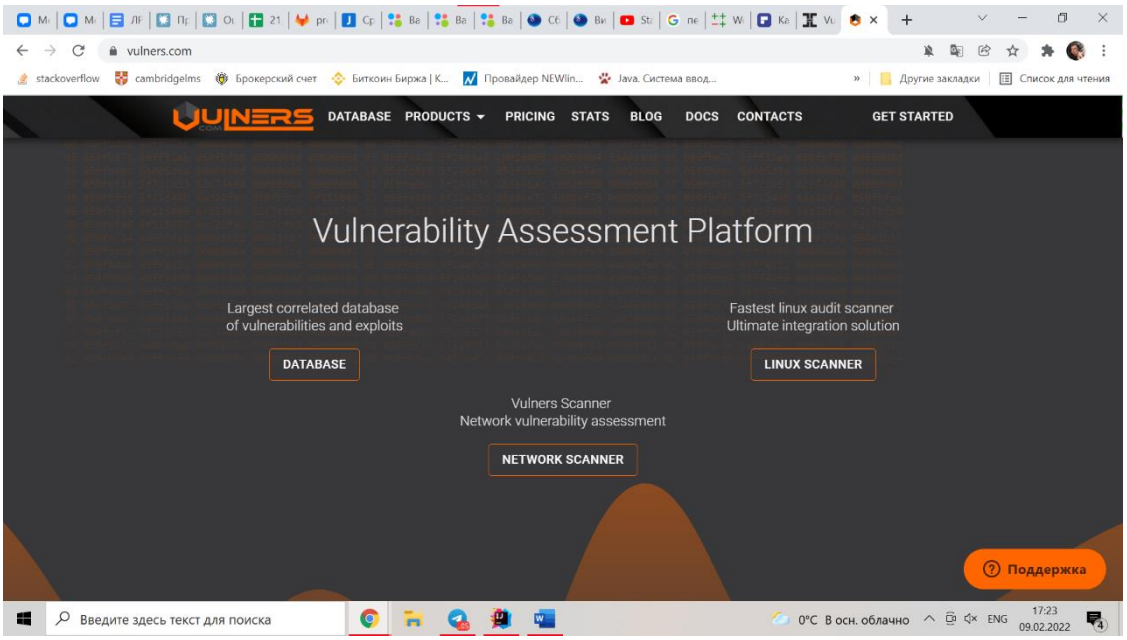
Vulners — это очень большая и непрерывно обновляемая база данных ИБ-контента. Сайт позволяет искать уязвимости, эксплоиты, патчи, результаты bug bounty так же, как обычный поисковик ищет сайты.

Vulners агрегирует и представляет в удобном виде шесть основных типов данных:

• Популярные базы уязвимостей. Они содержат общие описания уязвимостей и ссылки на источники. Например, известная CVE американского агентства MITRE и института NIST. Но, помимо информации из нее, в Vulners добавляются общие описания уязвимости и других исследовательских центров и центров реагирования: Vulnerability Lab, XSSed, CERT, ICS, Zero Day Initiative, Positive Technologies, ERPScan.

• Вендорские бюллетени безопасности. Это баг-репорты, которые пишут сами вендоры об уязвимостях в своих продуктах. Сейчас это разнообразные дистрибутивы Linux (Red Hat CentOS, Oracle Linux, Arch Linux, Debian, Ubuntu, SUSE), FreeBSD, сетевые устройства (F5 Networks, Cisco, Huawei, Palo Alto Networks) и популярные и критичные программы (OpenSSL, Samba, nginx, Mozilla, Opera), в том числе и CMS (WordPress, Drupal).

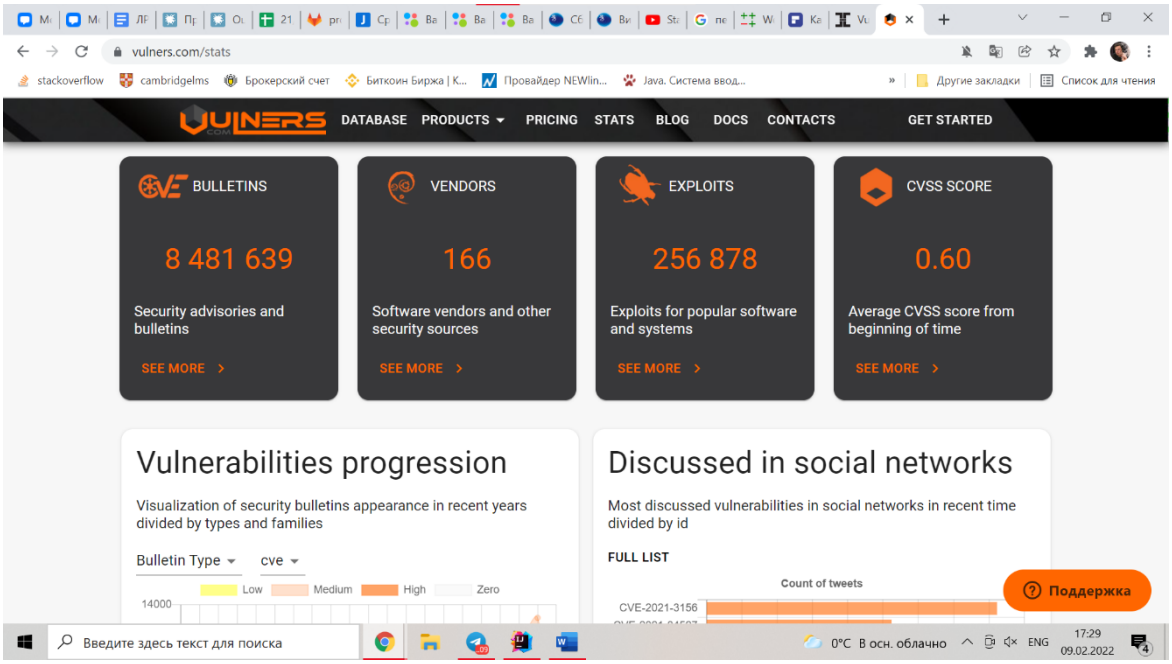
• Эксплоиты из Exploit-DB и Metasploit. Они парсятся и сохраняются полностью, с исходниками (их можно сразу смотреть в удобном редакторе).



• Nessus-плагины для детекта уязвимостей. Легко посмотреть, можно ли найти ту или иную уязвимость при сканировании сети этим популярным сканером.

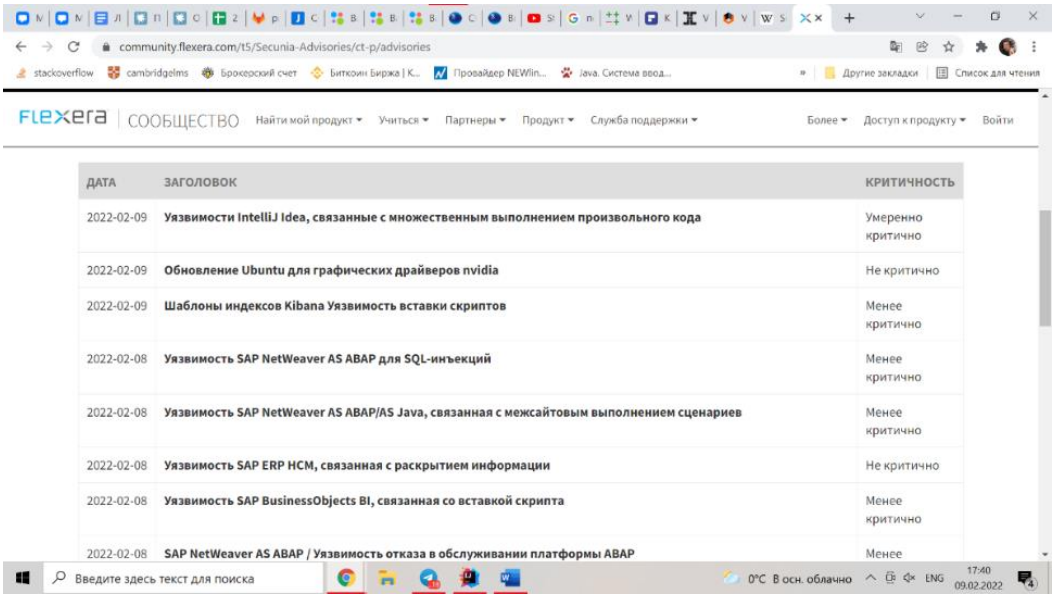
• Дисклозы багов с сайтов bug bounty программ. В Vulners поддерживаются записи с HackerOne.

• Публикации на тематических ресурсах. Собираются данные с Threatpost и rdot.org, где часто освещают темы, связанные с уязвимостями.



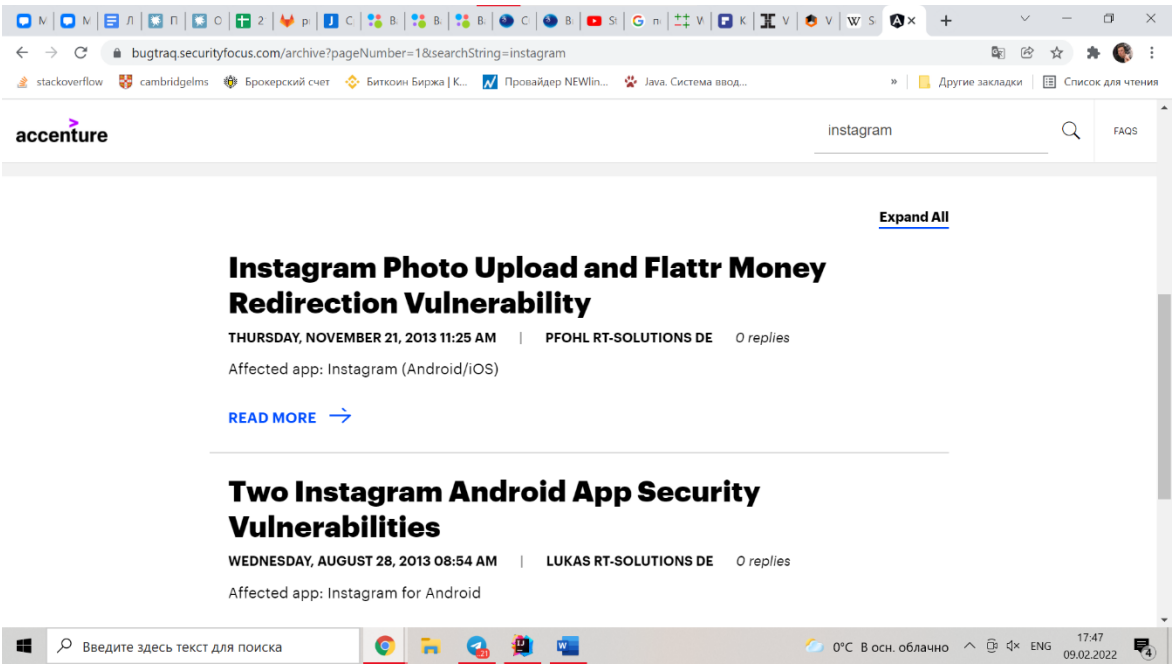
3. **Secunia**

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. Предлагает услуги платной подписки на базу уязвимостей.



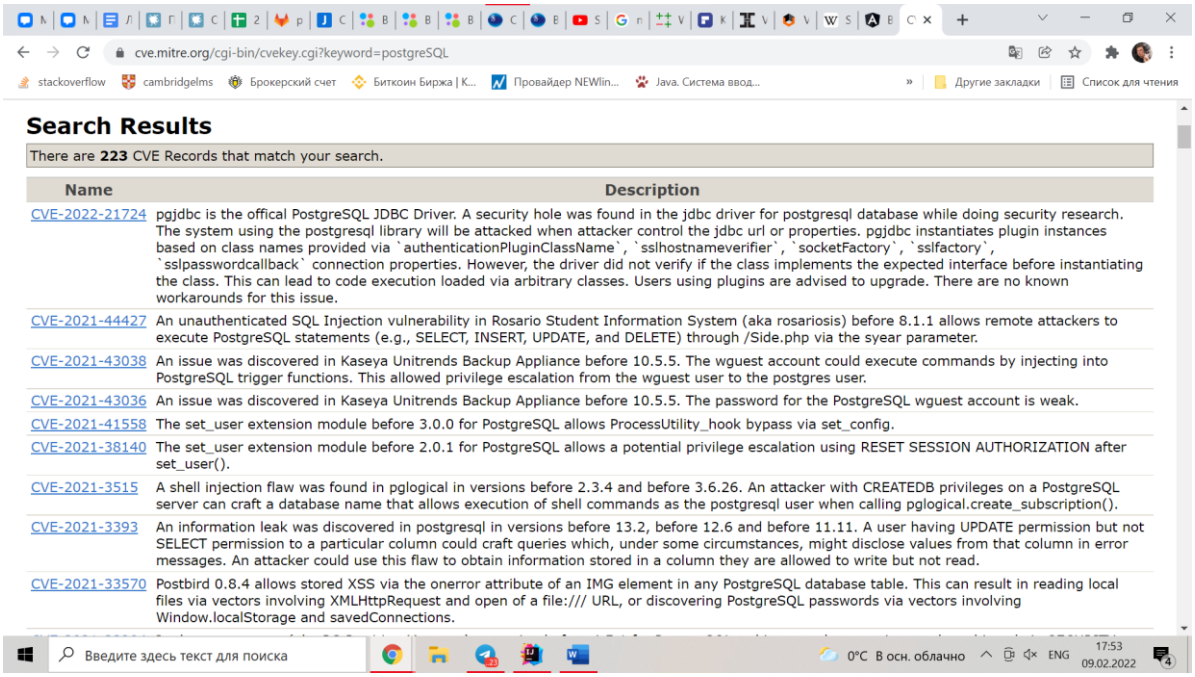
4. SecurityFocus

SecurityFocus был новостным онлайн- порталом компьютерной безопасности и поставщиком услуг информационной безопасности. Среди обозревателей и писателей SecurityFocus, где находится известный список рассылки Bugtraq , были бывший прокурор Министерства юстиции по киберпреступлениям Марк Раш и хакер, ставший журналистом Кевин Поулсен.



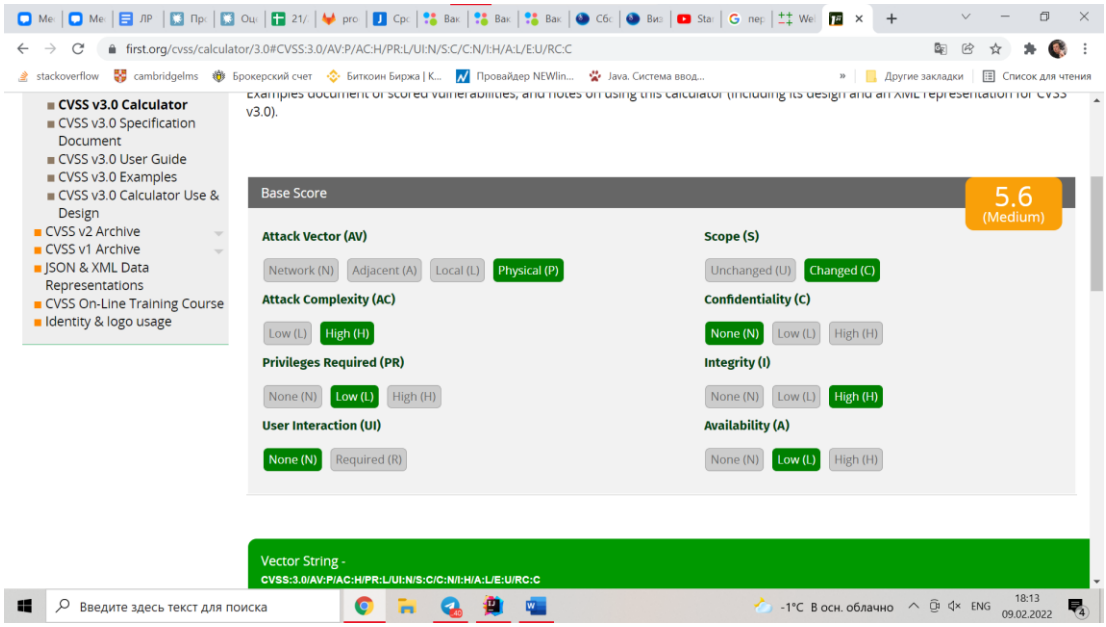
5. CVE

CVE — база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием. Поддержкой CVE занимается организация MITRE. Финансированием проекта CVE занимается US-CERT.



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

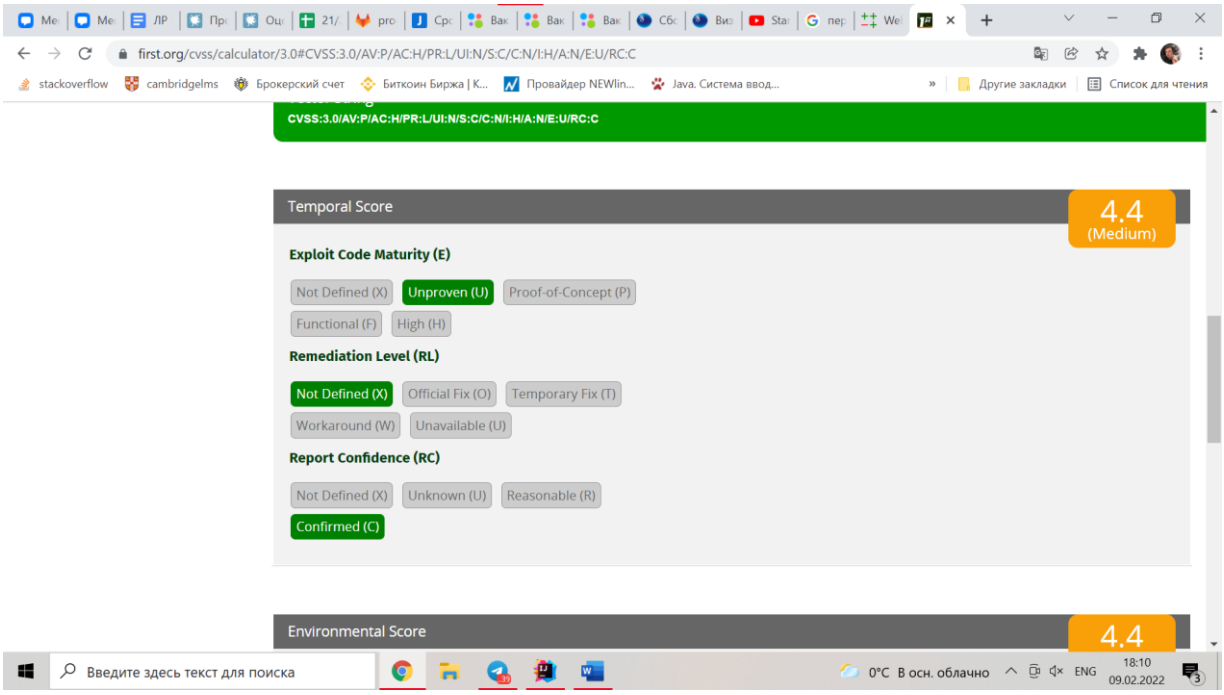
b) атака высокой сложности будет проводиться на физический уровень системы, при этом оказывается влияние на другие компоненты системы. Однако атака приводит только к нарушению целостности высокого уровня и доступности низкого. Взаимодействие с пользователем не требуется, а уровень привилегий - низкий.



Ответ: AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:L – 5.6

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

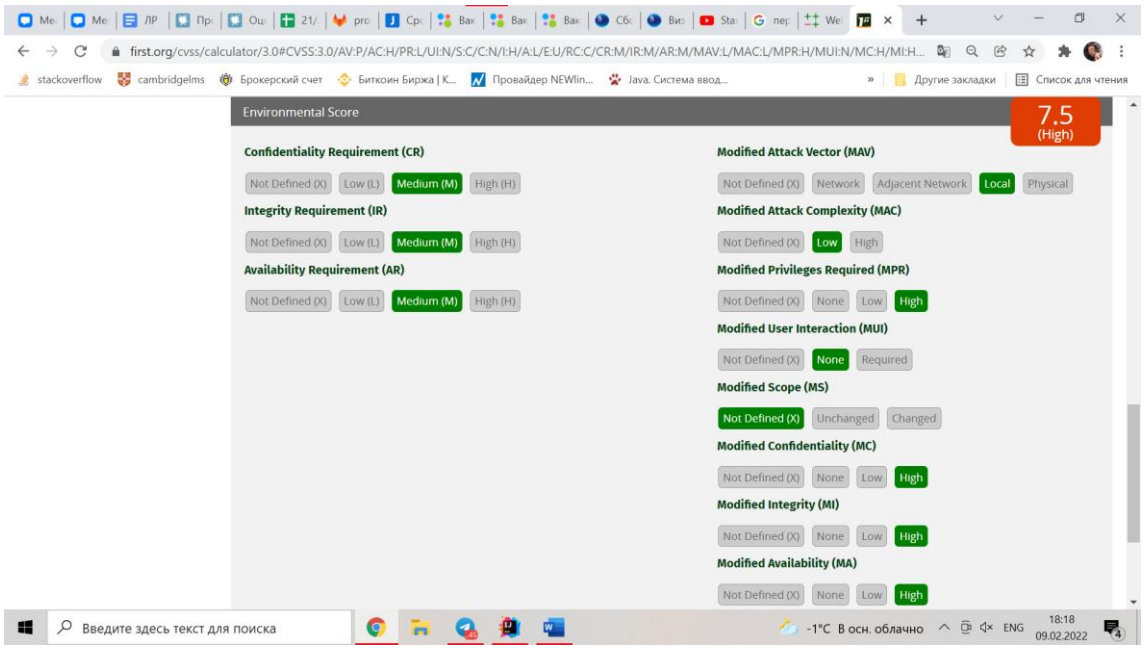
b) Предполагается, что есть сценарий для средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.



Ответ: E:U/RL:X/RC:C – 4.4

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

b) К уровню обеспечения КЦД заданы средние требования, однако влияние 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.



Ответ:

CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:H/MUI:N/MS:X/MC:H/MI:H/MA:H - 7.5

Вывод:

в результате проделанной работы я изучил метрики CVSS (Common Vulnerability Scoring System), познакомился с основными БД угроз и уязвимостей и узнал о трех китах информационной безопасности (КЦД).