Задача 1. Посчитать значение вектора уязвимости CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N согласно стандарту CVSS версии 3.1. *(12 баллов)*

Задача 2. Опишите значения метрик вектора уязвимости CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N. *(9 баллов)*

Задача 3. Посчитать оценку окружения уязвимости с учетом следующих значений метрик окружения CVSS:3.1/MAV:A/MAC:H/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:L/A:H/E:F/RL:O/RC:C. *(13 баллов)*

Задача 4. По описанию атаки составить базовый вектор уязвимости CVSS версии 3.1 и посчитать его значение. Microsoft Internet Explorer с 9 по 11 версию некорректно обрабатывает объекты в памяти, что позволяет атакующему выполнить произвольный код на системе при переходе пользователя по ссылке, содержащей вредоносный код. Злоумышленник может выполнить данную атаку удаленно. *(15 баллов)*

Задача 5. Определить какая из уязвимостей критичнее. Проверить правильность с помощью расчета значения вектора CVSS.

А) Алгоритм аутентификации в кардиостимуляторах Abbott Laboratories, изготовленных до 28 августа 2017 г., который включает ключ аутентификации и отметку времени, может быть скомпрометирован или обойден, что может позволить злоумышленнику, находящемуся поблизости, передать несанкционированные команды кардиостимулятору через радиочастотную связь.

Б) Эта уязвимость позволяет удаленным злоумышленникам выполнить произвольный код на уязвимых установках Google Chrome. Для использования этой уязвимости требуется взаимодействие с пользователем, поскольку жертва должна посетить вредоносную страницу или открыть вредоносный файл. Конкретный недостаток существует в обработке изображений JPEG 2000. Специально созданное изображение JPEG 2000, встроенное в PDF-файл, может заставить Google Chrome записывать в память за пределами выделенного объекта. Злоумышленник может использовать эту уязвимость для выполнения произвольного кода в контексте текущего процесса.
Злоумышленник создает PDF-файл, содержащий вредоносное изображение JPEG 2000. Это делается доступным для жертв, например, через веб-страницу. Жертва открывает PDF-документ в браузере Google Chrome, и браузер отображает PDF-файл с помощью встроенного средства просмотра PDFium PDF. Это включает эксплойт и запускает исполняемый код, который злоумышленник поместил в образ, захватывая браузер. *(20 баллов)*

Проектная задача. Итоговый показатель критичности не всегда определяется метриками CVSS. Также данный метод плохо подходит для производственных объектов, так как не учитывает физические составляющие системы. Предложите свою идею оценки рисков и методику ее расчета. Для корректной оценки задания необходимо привести примеры расчета. *(31 балл)*