**ПРАКТИЧЕСКАЯ РАБОТА №1**

**«ТЕКСТОВЫЙ ПРОЦЕССОР WORD»**

**Цель работы**

Исследовать основные функциональные возможности текстовых процессоров при подготовке документов, получить навыки создания документов c помощью MS Word (Writer/Libre Office). Освоить приемы работы с таблицами, формулами и диаграммами.

**Ход работы**

1. Создадим текстовый файл MS Word и сохраним на жестком диске под уникальным именем.



Рисунок 1 – Новый текстовый файл

1. Скопируем через «Буфер обмена» из Интернета небольшой фрагмент текста. Отредактируем его по инструкции из методических указаний.

Σ С начала ~~августа~~ 2021 года российский финансовый рынок подвергается постоянным масштабным DDoS-атакам. При этом злоумышленники продолжают планомерно увеличивать количество и интенсивность атак, а также применять не только хорошо известные, но и самые новые их типы.

В августе ФинЦЕРТ отметил череду масштабных DDoS-атак не менее чем на 12 крупных российских банков, процессинговых компаний и интернет-провайдеров. Запросы шли из США, Латинской Америки и Азии, сообщали СМИ. В начале сентября российский финансовый сектор вновь атаковали: под влияние попали крупные банки и телеком-операторы, предоставляющие им услуги связи.

Отдельный интерес к российской банковской сфере среди киберпреступников эксперты начали отмечать еще в середине лета 2021 года. В июле Банк России сообщал в СМИ о рисках «заражения» финансовых учреждений через участников их экосистем. На конференции Cyber Polygon 2021, прошедшей в июле, эксперты в области информационной безопасности Тереза Уолш (Teresa Walsh) и Троелс Оертинг (Troels Oerting) отмечали, что вектор атак смещается в сторону сторонних поставщиков организаций, через которые совершается до 40% атак.

С 9 августа российский центр мониторинга киберугроз (SOC) международного сервис-провайдера Orange Business Services фиксирует резкий рост количества запросов. Пытаясь достигнуть своей цели, преступники увеличивают их частоту, площадь адресного пространства и мощность.

Кроме того, злоумышленники комбинируют не только хорошо известные векторы атак, такие как TCP SYN, DNS Amplification, UDP Flood и HTTPS Flood, но и только недавно обнаруженные, например, DTLS Amplification. Этот тип атак был впервые замечен в конце 2020 года и начал широко применяться в середине этого года. Он использует уязвимости в серверах Citrix, и даже небольшая ботнет-сеть способна проводить большую по мощности атаку.

В общей сложности за месяц, с 9 августа по 9 сентября 2021 года, зафиксировано более 150 атак. При этом их интенсивность постоянно нарастает. В докладе ФинЦЕРТ по итогам 2020 года отмечалось, что самая мощная атака в 2019-2020 годах велась с интенсивностью 49 Гбит/с (на 2 Гбит/с выше рекорда 2018 года). Уже в августе 2021 года SOC Orange Business Services отбивал запросы мощностью 100 Гбит/с, а 6 сентября этот показатель превысил 150 Гбит/с. Преступники пытаются постоянно увеличивать мощность атак в надежде, что телеком-провайдеры не смогут провести очистку трафика в столь больших объемах.

Злоумышленники также использовали вектор HTTPS Flood для невозможности использования приложения банков, в этом случае атака совершалась с IP-адресов России, Украины и Франции. В других случаях были задействованы ботнет-сети из Тайваня, Индонезии, Китая, России и США.

Увеличивается площадь атакуемого адресного пространства: если в августе фиксировались в основном адресные запросы на конкретные IP-адреса финансовых организаций, то с сентября проводятся атаки, затрагивающие 256 и более адресов за раз. При этом преступники постоянно меняют или комбинируют типы атак для увеличения сложности их отражения. Весь август финансовый рынок имел дело с векторами HTTPS и DNS Amplification, 31 августа к ним добавились атаки TCP SYN, а 2 сентября были зафиксированы векторы IP Fragmentation и DTLS Amplification. Неоднократно фиксировались сразу несколько типов атак, одновременно совершаемых на финансовые организации: к примеру, атака с целью переполнения магистрального канала связи шла параллельно запросам в зашифрованном трафике на сервис платежей.

«По тому, как настойчиво и изобретательно действуют киберпреступники, можно говорить, что мы имеем дело со сложной спланированной акцией, направленной на дестабилизацию как минимум российского финансового рынка. В ответ на эту волну атак мы расширили функционал собственной системы автоматизации защиты от DDoS, сократив время от обнаружения атаки до реакции на нее до нескольких секунд. Дополнительно мы подключаем наиболее подверженных DDoS клиентов к мощностям нашего центра очистки во Франкфурте, способного выдержать атаку до 5 Тбит/c», — говорит операционный директор Orange Business Services в России и СНГ Ольга Баранова.

1. Создадим таблицу согласно шаблону из методических указаний и введём в неё произвольные значения баллов, полученных студентами на сессии. Далее с помощью формул рассчитаем сумму баллов каждого ученика и средние значения по дисциплинам. Сделаем выводы по полученным значениям.

**Ведомость оценок студентов**

Таблица 1 – Ведомость оценок студентов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Фамилия | Название дисциплины | | | | Сумма |
| Математика | История | Физика | Программирование |
| 1 | Карпов | 5 | 4 | 3 | 4 | 16 |
| 2 | Иванов | 4 | 3 | 4 | 5 | 16 |
| 3 | Кузнецов | 3 | 3 | 2 | 2 | 10 |
| 4 | Сидоров | 2 | 3 | 3 | 3 | 11 |
| 5 | Рыбин | 4 | 4 | 3 | 4 | 15 |
| Итого | | 18 | 17 | 15 | 18 | 68 |
| Средн. оценка | | 3,6 | 3,4 | 3,0 | 3,6 | 13,6 |

По результатам сессии не выявлено ни одного отличника или хорошиста. Ни по одной из дисциплин средний балл не превышает 3.6, вследствие чего результаты сессии можно считать неудовлетворительными.

1. Введём формулу из методических указаний (вариант 1.4.1).
2. Построим диаграмму по созданной таблице (таблица 1). На диаграмме отобразим балл каждого из студентов по каждой из дисциплин.
3. Нарисуем структурную схему цикла «while do» с помощью инструмента «Фигуры».

условие

+

оператор

Рисунок 2 – Блок-схема

**Вывод**

В ходе работы были использованы различные инструменты текстового процессора «Microsoft Word». С их помощью в одном текстовом файле были созданы текст, включающий в себя различные способы выделения и разметки, таблица с формульными значениями, формула, созданная с помощью инструмента «Формулы», диаграмма по значениям из таблицы и рисунок, созданный с помощью инструмента «Фигуры».

По окончании работы были получены новые и закреплены уже ранее имеющиеся навыки работы с основными функциями текстового процессора операционной системы Windows «Microsoft Word».