Таким образом, проведённое исследование показало, что эффективность синхронизации древовидных машин четности зависит от конфигурации их структурных параметров. Для систем, работающих в условиях сетевых задержек, оптимальной стратегией является использование умеренных значений *K* и *L* при максимально возможном значении *N*, которое позволяет вычислительная мощность устройств. Увеличение *N* обеспечивает кратный рост скорости генерации ключа и повышение криптостойкости, практически не увеличивая количество итераций обмена, что важно при нестабильном соединении. В то же время, чрезмерное увеличение параметра L ведет к недопустимому росту времени синхронизации.

## Список использованных источников

1. Юрченков Иван Александрович, Лищенко Тимофей Викторович Синхронизация древовидных машин четности // Universum: технические науки. 2024. №5 (122).

2. Ушаков Андрей Константинович Выбор оптимальной конфигурации древовидных машин четности при их использовании для генерации секретного ключа шифрования // Научный журнал. 2018. №6

3. Урбанович, П. П. Нейросетевые технологии в криптографических приложениях : [монография] / П. П. Урбанович, М. Д. Плонковски, М. Долецки. – Минск : БГТУ, 2024. – 221 с.

УДК 681.3:553.98(574.4)

**А.А. Овезова, К.Р. Аннамухаммедов, Д.М. Агаева, Е.Т. Язлыев**
Международный университет нефти и газа имени Ягшыгельди Какаева,
Ашхабад, Туркменистан

# РАЗРАБОТКА СИМУЛЯТОРА КИБЕРАТАКИ ЧЕРЕЗ МНОГОПОТОЧНУЮ РЕЗИДЕНТНУЮ ПРОГРАММУ

***Аннотация.*** *Статья описывает создание симулятора кибератаки, работающего в виде многопоточной резидентной программы, имитирующей устойчивые вредоносные процессы. Представлены механизмы взаимной защиты потоков, особенности удаления и применение в обучении кибербезопасности. Симулятор позволяет формировать практические навыки противодействия атакам.*

**A.A. Ovezova, K.R. Annamuhammedov,**
**D.M. Agayeva, Ye.T. Yazlyyev**
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

# DEVELOPMENT OF A CYBERATTACK SIMULATOR VIA A MULTITHREADED RESIDENT PROGRAM

***Abstract.*** *The article describes the development of a cyberattack simulator implemented as a multithreaded resident program reproducing persistent malicious behavior. It outlines interprocess protection mechanisms, removal strategies, and educational applications. The simulator helps students acquire practical cybersecurity skills.*

Все больше внимания в настоящее время уделяется способам и технологиям обучения слушателей навыкам кибербезопасности. Особо популярными в наше время являются симуляторы различных атак и угроз. Данные программы и продукты совмещают в себе как создание и проведение искусственных атак, так и их удаление и восстановление системы с оценкой проделанной слушателем работы.

В данной работе была поставлена задача разработать трёхпоточный резидентный симулятор кибератаки.

Цель программы – создать симуляцию атаки, которая после запуска в операционной системе Windows начинает работать по трём паралельным потокам, причём каждый поток защищает дригие. Рассмотрим работу созданного симулятора [1].

При запуске (например, Project1.exe или test.exe) программа работает в фоновом режиме. Ее нельзя увидеть обычным способом. Для обнаружения нужно открыть диспетчер задач (сочетание Ctrl+Alt+Delete) и перейти в вкладку "Сведения" (Рис. 1).

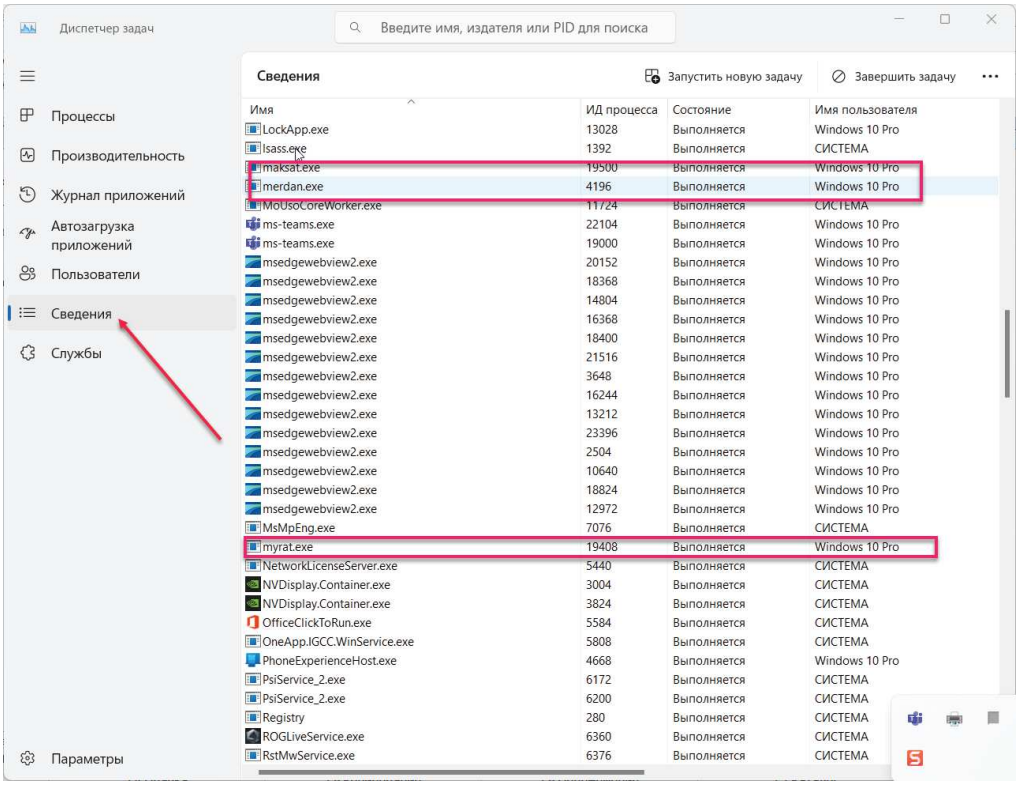


**Рис.1- Загрузка потоков в оперативную память**

Как видно на изображении, существует три таких потока (фактически их четыре, включая test.exe, но он служит только загрузчиком и не выполняет никаких других действий). Мы поочерёдно выбираем их и нажимаем кнопку "Снять задачу", чтобы завершить процессы. Однако после удаления последнего потока он снова восстанавливается. Так-как другие два потока остаются рабочими.

Эти потоки постоянно восстанавливают друг друга (например, поток maksat восстанавливает потоки myrat и merdan). Поэтому удалить их обычным способом невозможно. Чтобы завершить их работу, необходимо удалить два процесса одновременно с очень высокой скоростью.

Основные характеристики этих потоков:

а) Они (их физические файлы) находятся в отдельных папках внутри директории "TEST".

а) Запускаются через ключ реестра.

б) Защищены от стандартного удаления.

в) Поддерживают друг друга, проверяя состояние каждую миллисекунду. Если один из процессов будет удалён, остальные его немедленно восстановят.

После кибератаки, данные потоки оставляю в системе вредоносные следы:

а) Диспетчер задач заблокирован.

б) Редактор реестра заблокирован.

в) MS Word заблокирован.

г) Рабочий стол заблокирован.

д) На панели задач вместо часов отображаются посторонние символы.

е) Локальные диски скрыты.

ж) Клавиатура и мышь отключены.

з) В текстовых полях автоматически удаляется текст и вводятся другие символы.

Удалить эти процессы стандартными методами невозможно. Однако с помощью Комплекса защиты от кибератак или утилиты Turkmen Cyber Hack, разработанной в одном пакете с данным симулятором творческой группой Университета, можно устранить данную угрозу [2].

Способ удаления вредоносных процессов:

В программе Turkmen Cyber Hack необходимо:

Выбрать соответствующие процессы по имени и ID.

Через контекстное меню добавить их в Список процессов для удаления.

После этого их имена и ID будут записаны в Дополнительный список удаления процессов и уничтожены (Рис 2.).

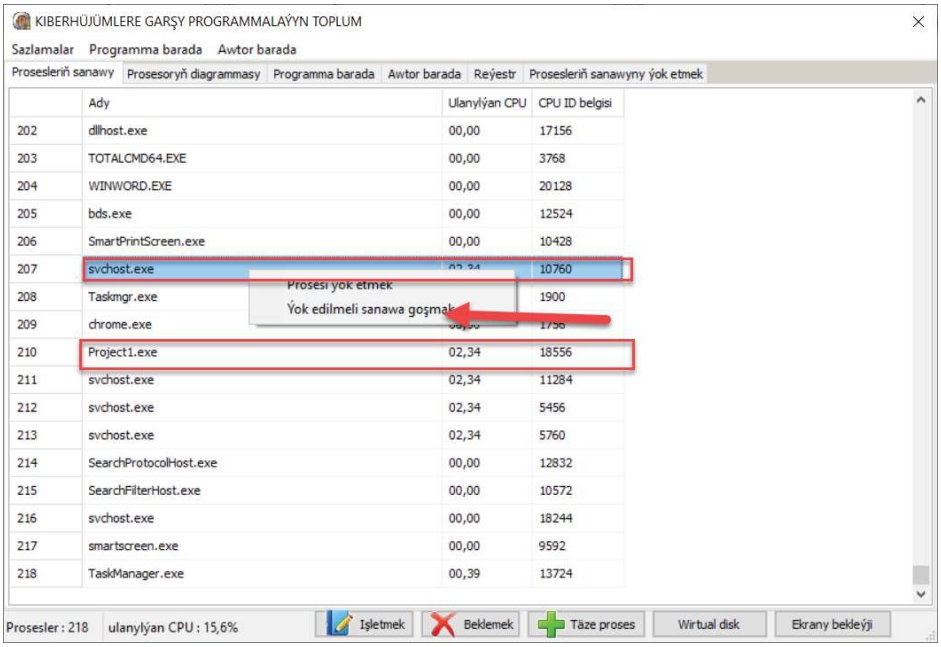


**Рис.2 - Загрузка потоков в список для удаления.**

После выбора всех процессов и выполнения вышеуказанных шагов необходимо перейти к Вкладке удаления списка процессов.

В данной вкладке при нажатии на кнопку "Удалить" или "Отключить резиденты", указанные процессы будут удалены из списка и оперативной памяти.

Симулятор был создана в скрытом резидентном режиме. После запуска она создает три независимых друг от друга (на первый взгляд) резидентных процесса в оперативной памяти: "maksat", "merdan" и "myrat".

Эти процессы постоянно следят друг за другом. Если один из них завершается, оставшиеся два моментально его восстанавливают.

В коде программы используется быстро выполняемый ассемблерный код, что делает её крайне устойчивой к стандартным методам удаления.

Для полного устранения этих процессов требуется программа с высокой скоростью обработки, способная одновременно уничтожить все три процесса, прежде чем они успеют восстановиться [3].

Данный симулятор хорошо зарекомендовал себя в учебном процессе при подготовке специалистов по кибербезопасности. Он позволяет успешно бороться с паническими состояниями у тестируемых, а также вырабатывает навыки принятия быстрых и правильных решений.

### Список использованных источников

6. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д.А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.: ил.

7. "Possible Minds: Twenty-Five Ways of Looking at AI" by John Brockman (Editor) (2019).

8. M.Çuriýew, R.Mahmudow, J.Geldiýew. Kiberhowpsuzlyk. Ýokary okuw mekdepleri üçin okuw gollanmasy. A.: “Ylym”, 2023ý. – 340 s.

УДК 659.1

**К.А. Павлинова**
Новосибирский государственный университет экономики и управления
Новосибирск, Россия

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ОСОБЕННОСТИ РЕКЛАМЫ В СФЕРЕ ТУРИЗМА: ЦЕЛИ, ЗАДАЧИ И ЭТАПЫ РАЗРАБОТКИ РЕКЛАМНОГО СООБЩЕНИЯ