УДК 681.3:553.98(574.4)

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ПО ОТРАЖЕНИЮ КИБЕРАТАК

Д. М. АГАЕВА, М. А. ГЕЛЬДИЕВА, Д. Д. ЧАРЫЕВА
(Международный университет нефти и газа имени Ягшыгелди Какаева, г. Ашхабад, Туркменистан);

Б. С. ГАФУРОВ
(Драгон Ойл Лтд, г. Ашхабад, Туркменистан)

Аннотация. *В статье рассматривается разработка и применение программного обеспечения против уже разросшейся кибернетической атаки. Авторы описывают возможности программы в контексте возможной угрозы на ту или иную системную службу или функцию операционной системы Windows.*

Ключевые слова: *кибербезопасность, кибератака, программное обеспечение, системные службы, системный реестр.*

Киберпространство состоит из множества компьютерных систем, соединённых в одну сеть и интегрированных телекоммуникационных систем. Оно стало одной из характерных черт современного общества, обеспечивая и расширяя высокоскростную связь, функционирование распределённых систем управления и контроля, хранение и передачу больших объёмов данных и функционирование распределённых систем [3]. Повсеместное распространение взаимосвязанных систем создало такую степень зависимости и уязвимости среди отдельных лиц, отраслей промышленности и правительств, которую трудно прогнозировать, контролировать и предотвращать [1]. Информационная безопасность стала одной из главных проблем современного мира, требующей внимания и реакции со стороны отдельных лиц, частного бизнеса, неправительственных организаций, а также международных институтов и органов [2].

Безопасность в киберпространстве должна быть направлена на обеспечение защиты данных и трафика. Поэтому остановимся очень кратко на понятии киберпространства. Чтобы обеспечить ясность определений, мы опирались на определение киберпространства, данное Национальным институтом стандартов и технологий США: «взаимозависимая сеть инфраструктур информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры...». Основное содержание киберпространства заключается в деятельности пользователей цифровых информационных ресурсов и инфраструктуры информационно-коммуникационных технологий (ИКТ).

Таким образом, там, где мы в повседневной жизни сталкиваемся с ИКТ, там же может осуществляется деятельность под обобщающим названием «кибервойны». Средством боевого воздействия в кибервойнах является программный код, нарушающий работу, выводящий из строя, либо обеспечивающий перехват управления различного рода материальными объектами и сетями, оснащенными электронными системами управления. Кибернетическая война состоит из двух этапов.

Первым этапом является шпионаж. Первый этап подразумевает сбор данных, посредством взлома сетей и информационных систем компаний, организаций и даже государств.

Вторым этапом является сама кибератака. Атаки различаются в зависимости от целей и задач действий.

Существует множество методов и технологий противодействия и предотвращения кибератак, их сложность и эффективность зависят от профессионализма разработчиков, и конечно же от материального обеспечения. Не секрет, что самый эффективный способ борьбы с киберугрозами это профилактика и принятие мер на самых ранних стадиях начавшейся кибератаки.

Однако в данной работе рассматривается вопрос противодействия уже начавшейся и продолжающейся по всем направлениям кибератаке. Для этого нами было разработано специальное программное обеспечение, которое способно решить многие вышеупомянутые вопросы, и в случае необходимости полностью подавить и исправить последствия кибератаки.

Программное обеспечение разработано в виде стандартного приложения Windows (рисунок). Состоит оно из нескольких сегментов, осуществляющих свои функции независимо от друг-другу [3, 4].

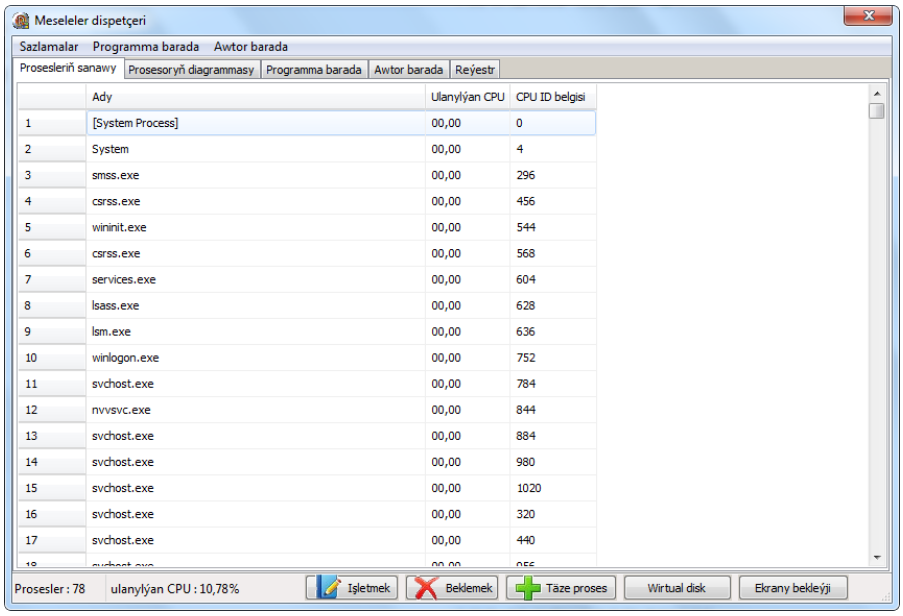

Рисунок. – Внешний вид программы

Рассмотрим работу этих сегмент.

Первый (основной) сегмент – отображение списка запущенных программ. В этом списке можно завершить любую выбранную программу или отправить ее список удаляемых процессов.

Второй сегмент – графическое отображение загрузки процессов в виде диаграммы, которая позволяет определить процессы, которые выходят за рамки обычной активности и таким образом подпадают под список подозрительных и потенциально опасных потоков.

Третий сегмент – чтение в альтернативном режиме системного реестра и настройка списка программ, загружаемых наряду с системой. Этот сегмент позволяет проводить профилактику запуска или загрузки процессов и выявить подозрительные команды.

Четвертый сегмент – запуск утилиты для ограничения или разрешения запуска определённых процессов и программ, которая позволяет нейтрализовать и блокировать потенциально вредоносную программу.

Пятый сегмент – защита носителем флэш экрана и возможности входа в систему, в результате экран блокируется полноэкранным режимом окна с игнорированием и перехватом сообщений операционной системы по закрытию данного окна, а на определенный флэш-носитель записывается информация (пароль), необходимый для разблокировки экрана. При вставке флэш-носителя в USB разъем, автоматически считывается пароль, если он есть и пароль совпадает, то экран разблокируется, а если файла с паролем нет или он не совпадает (вставлен другой флэш носитель) экран остаётся заблокированным.

Шестой сегмент – создание виртуальных дисков на носителях информации с возможностью сохранения в них необходимых данных защищенных паролем и шифрованием. С помощью этого сегмента можно сохранять данные на виртуальном диске, пространство которого расположено на флеш-носителе, которое впоследствии автоматически кодируется, когда флеш-носитель извлекается от USB-разъема.

Седьмой сегмент – запускает список удаляемых программ, а также команду по мгновенному удалению данных процессов, это очень полезная утилита в случаях, когда вредоносная программа действует поточно (т.е. ее процессы поддерживают друг-друга не позволяя удалять их обычным способом).

Рассмотренные выше функции и возможности этой программы, дают возможность успешно и эффективно отражать некоторые существующие виды кибератак, обеспечить стабильность компьютерной системы. Разработанное программное обеспечение может быть использовано на любом государственном и частном предприятии и учреждении для самостоятельной защиты пользователем своей компьютерной системы от внешних угроз. На эту программу в соответствующем порядке был получен патент (№ 88).

ЛИТЕРАТУРА

1. Сикорски М., Хониг Э. Вскрытие покажет! Практический анализ вредоносного ПО. – СПб.: Питер, 2018. – 768 с.: ил. – (Серия «Для профессионалов»).
2. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д.А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.: ил.
3. Министерство национальной обороны. Кибербезопасность: Типовой учебный план (УП), 2016.
4. M.Çuriýew. Maglumatlaryň gory we banklary. Ýokary okuw mekdepleri üçin okuw kitaby. – A.: „Ylym“ neşirýaty, 2015.
5. Архангельский А.Я. Программирование в Delphi. – М.: БИНОМ, 2008.