УДК 681.3:553.98(574.4)

НЕКОТОРЫЕ ПРОБЛЕМЫ ПОДГОТОВКИ КВАЛИФИЦИРОВАННЫХ СПЕЦИАЛИСТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Б. Я. АТАМАНОВ, М. Ч. ХЫДЫРОВ, М. М. ЧУРИЕВ, А. Д. ЯЗМУРАДОВ
(Международный университет нефти и газа имени Ягшыгелди Какаева, г. Ашхабад, Туркменистан)

Аннотация. *В данной работе рассматриваются вопросы разработки и применения симулятора пассивной и активной угрозы для подготовки квалифицированных кадров в области информационной и кибербезопасности. Симулятор предназначен для искусственного создания условий, приближенных к реальным условиям кибератаки. Система снабжена также, мониторингом, для автоматизированной проверки и создания отчета по выполненной будущими специалистами по кибербезопасности работе.*

Ключевые слова: *кибербезопасность, симулятор кибератаки, пассивная угроза, активная угроза.*

О проблемах обеспечения кибербезопасности в современном мире рассказано и написано достаточно много. Дается много рекомендаций, разрабатываются стратегии и политики обеспечения кибербезопасности. Можно с уверенностью сказать, что ни одну из них нельзя воплотить в жизнь без тщательного изучения и анализа источника киберугроз, без изучения природы самой кибератаки.

Поэтому в настоящее время кибербезопасности уделяется не меньше времени, чем непосредственно цифровым технологиям. Основная проблема в сфере кибербезопасности – это дефицит квалифицированных кадров. Это связано еще с примечательной особенностью рассматриваемой сферы – порог вхождения в квалификацию один из самых высоких, в тоже время для становления киберагрессором особой квалификации и не нужно [1].

В этой статье в процессе разработки симулятора многоволновых кибератак, мы постараемся оценить возможности потенциального киберагрессора, дать оценку масштабам возможной кибератаки, а также выработать рекомендации по предотвращению, выявлению и противодействию такого рода кибератак.

Чтобы побороть эту проблему развиваются различные виды подготовки специалистов по кибербезопасности, в том числе и конкурсные, когда дух соперничества благоприятно влияет на процесс приобретения навыков. В данной статье мы хотели бы поделиться своим опытом в проведении хакатона по обеспечению кибербезопасности. Для его проведения был использован специальный симулятор пассивных и активных киберугроз.

На языке объектно-ориентированного программирования, такого как например Delphi (можно любого другого), было разработано два программных обеспечения, запатентованных Государственной службой Туркменистана по интеллектуальной сосбственности.

Задача первой программы, заключается в автоматическом создании на компьютерах симуляций активных многоволновых угроз, искуссно замаскированных и скрытых в операционной системе.

В задачу второй программы входит размещение пассивных угроз и создание временных «неудобств» для участников, а также анализ состояния компьютера команд и автоматическая оценка на основании выявления следа угроз работ, проделанных со стороны команд.

Таким образом, каждой команде предоставляется один компьютер, «загруженный» пассивными и активными угрозами. Задача команд состоит в поэтапном выполнении следующих задач:

– своевременное определение и выявление активной угрозы и разрастающей кибератаки;

– остановка, нейтрализация а затем и дальнейшее удаление данной угрозы;

– предупреждение и своевременное обнаружение пассивной и потенциальной угрозы;

– автоматизация проделанных действий по устранению вышеуказанных угроз и кибератак и разработка на этой основе соответсвующего программного обеспечения.

Командам приходится действовать в непростых условиях, симулятор угроз искуссно расставляет ловушки, препятствует выполнению действий по устранению угроз, через определенные промежутки времени запускает новые волны атак, призванные запутать будущих специалистов по кибербезопасности. Нужно отметить еще тот факт, что действия команд стеснены тем обстоятельством, что им не разрешается осуществлять перезагрузку системы, менять системное время, восстанавливать систему, так-как данные действия в условях реальной угрозы, еще более усугубляли сложившую ситуацию или же приводили к потере пользовательских и системных файлов и данных. Созданный программный мониторинг при выявлении данных ситуаций автоматически штрафует команды, убавляя их баллы.

Таким образом, команды действуют в условиях, максимально приближенных к условиям с реальной киберугрозой.

На выполнение поставленной задачи, участникам отведено до 4 обязательных часа, в течении которых проходят волны атак и дополнительно 2 часа на разработку программного обеспечения по предупреждению, обнаружению, противодействию и устранению киберугроз.

Оба разработанных программных обеспечений, показали себя с хорошей стороны, а в особенности программа мониторинга кибератак, главное и единственное окно которой показано на рисунке 1.

Как видно из рисунка работа программы состоит из 4 блоков.

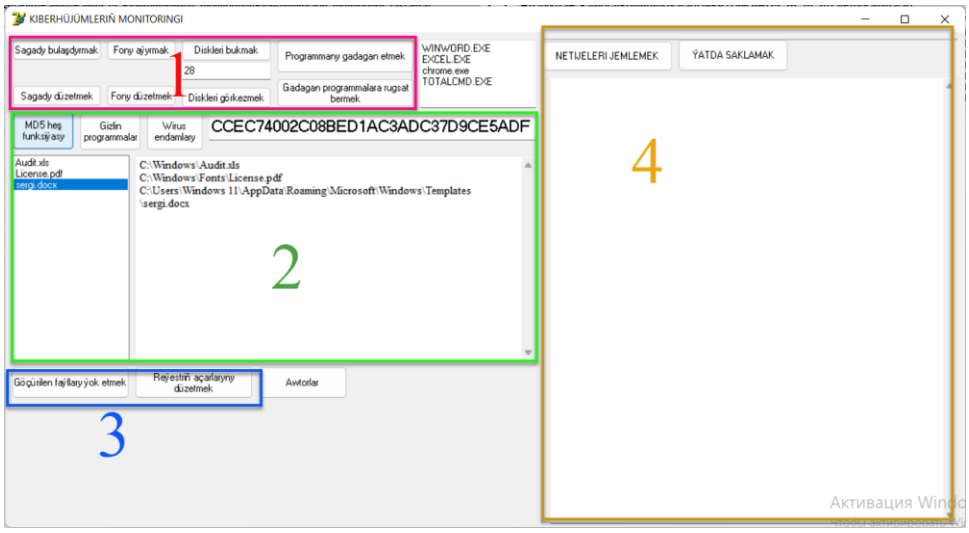

Рисунок 1. – Окно программы мониторинга кибератак

Первый блок устраивает различные временные неудобства, такие как изменение формата системного времени (когда вместо даты и текущего времени показывается указанный в программе текст), блокировка рабочего стола, скрытие локальных дисков и запрет указанных в списке приложений (Word, Excel, Chrome, Total Commander) [2]. Следует отметить, что в самой программе есть и «противоядие» для указанных «неудобств» – (кнопки, расположенные ниже).

Во втором блоке расположены кнопки, расставляющие по всей файловой системе пассивные киберугрозы (файлы с одинаковыми хеш-суммами, но с разными названиями и расширениями, скрытые программы и тела вирусов).

Третий блок, удаляет вышеуказанные файлы и восстанавливает нормальное состояние ключей системного реестра.

Четвертый блок является самым важным, так-как проводит мониторинг операционной системы на предмет устранения и ликвидации пассивных киберугроз и активных кибератак, исправления ключей реестра и сохранности пользовательских и системных файлов. Он оценивает по нескольким пунктам, работу проделанную на компьютере специалистами и выдает оценку в баллах, определяя таким образом победителей хакатона (рисунок 2).

Как показала практика, в том числе на примере данного хакатона, соревнования такого рода, более действенно позволяют выявлять творческий потенциал в IT области и развивать способность командной работы, которая более всего способствует решению различных задач в в области кибербезопасности.

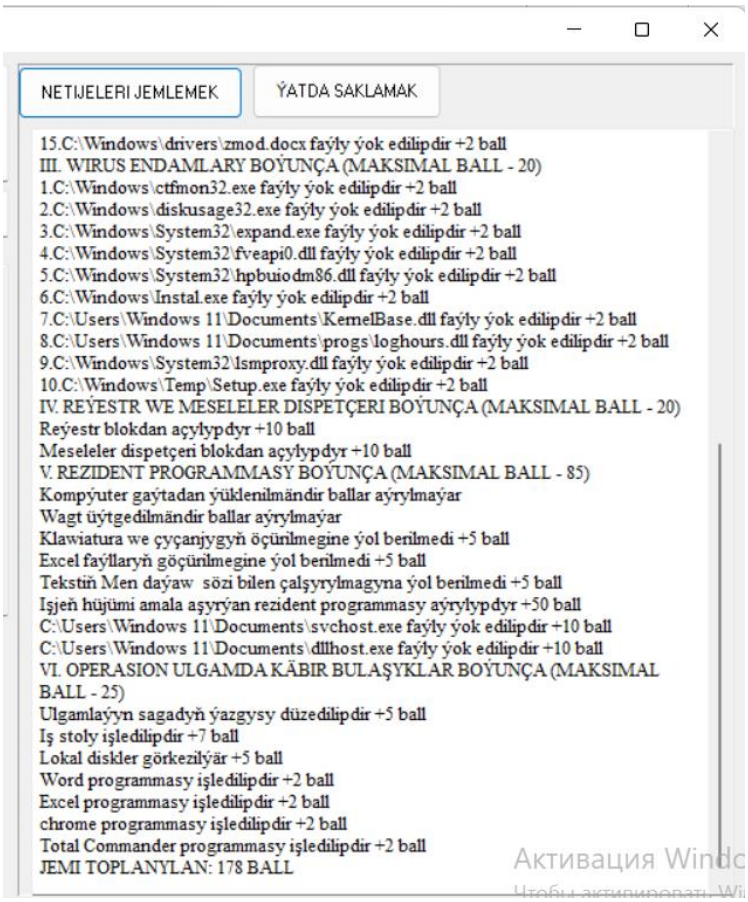

Рисунок 2. – Создание отчета о состоянии системы и проделанной работе по обеспечению кибербезопасности

Из всего выше сказанного следует, что киберагрессор обладает достаточно мощными средствами кибератаки, тем более он атакует первым и имеет возможность дезориентировать своих визави очередными волнами кибератак, действующих через определенные промежутки времени.

В стадии разработки данного симулятора, который несомненно будет очень полезен для подготовки специалистов в «боевых» условиях, был получены важный опыт, который будет полезен в дальнейшем для противодействия кибератак и который заключается в том, что в первую очередь нужно ликвидировать активную угрозу, т.е. резидентную программу (программы), иначе все предпринятые действия будут напрасными.

В результате проведения такого рода мероприятий, с применением упомянутых программ симулятора и мониторинга достигаются следующие цели и задачи, которые несомненно важны при подготовке высококвалифицированных кадров в области информационной и кибербезопасности:

- повышение качества профессиональной подготовки студентов;
- повысить креативность;
- формирование любви к своей профессии;

– создание различного целевого программного обеспечения;

– соединение различной информации в создаваемом программном обеспечении;

– определить пути повышения активности программ;

– раскрыть умения учащихся;

– создать для обучающихся в образовательном процессе реальные условия атак и опасностей и научить их преодолевать эти угрозы;

– научиться эффективно использовать все технические и программные ресурсы для своевременного выявления и обнаружения кибератак;

– обучение созданию программных средств обнаружения атак;

– обучение командной работы.

ЛИТЕРАТУРА

1. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013. – 206 s.
2. Архангельский А.Я. Программирование в Delphi. – М.: БИНОМ, 2008.