https://smmplanner.com/blog/nieirosieti-kak-ispolzovat-v-rieklamie-i-markietinghie-primiery-i-varianty/amp/. – Дата доступа: 05.11.2023.
3. Gutiérrez, A., Rodríguez, J. Artificial Intelligence in Marketing: On the Cutting Edge of Next Generation Marketing. Springer / Gutiérrez, A., Rodríguez, J. Artificial; – 2020: P. 271.

УДК 681.3:553.98(574.4)

М.М. Чуриев, А.Д. Язмурадов,
А.С. Мамметесенова, М.Ч. Хыдыров
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

РАЗРАБОТКА И ПРИМЕНЕНИЕ ПРОГРАММЫ МОНИТОРИНГА КИБЕРАТАК ДЛЯ ПРОВЕДЕНИЯ ХАКАТОНОВ ПО КИБЕРБЕЗОПАСНОСТИ

Аннотация. *В статье рассматривается проблема разработки программного обеспечения по мониторингу за пассивными киберугрозами и активными кибератаками, а также применение данной программы для проведения хакатонов по обеспечению кибербезопасности и оценки работ по устранению киберугроз.*

M.M. Churiyev, A.D. Yazmuradov,
A.S. Mammetesenova, M.Ch.Hydyrov
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

DEVELOPMENT AND APPLICATION OF A CYBER ATTACK MONITORING PROGRAM FOR CYBER SECURITY HACKATHONS

Abstract. *The article discusses the problem of developing software for monitoring passive cyber threats and active cyber attacks, as well as the use of this program for conducting hackathons to ensure cybersecurity and evaluating work to eliminate cyber threats.*

Повсеместность современных компьютерных систем и способность осуществлять связь или взаимодействовать с помощью различных средств, от мобильных устройств до носимых компьютеров, создают для государственных и негосударственных субъектов ряд

неотъемлемых уязвимостей и возможные векторы атак. Использование этих уязвимостей может привести к широким последствиям для национальной безопасности посредством таких намеренных действий, как шпионаж, снижение эффективности объектов командования и управления, кража интеллектуальной собственности и чувствительной информации личного характера, нарушение предоставление существенных услуг и функционирования критически важной инфраструктуры или нанесение ущербы экономике и промышленности [1].

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 [2].

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. Напомним, что хакатон - это соревнование между командами в IT-сфере, суть которого сводится к поиску решения заявленной проблемы в рамках какого-либо продукта.

Цели проведения данного мероприятия заключаются в следующем:

- 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.

В хакатоне Turkmen Cyber.Hack? проведенном в Международном университете нефти и газа имени Ягшыгелди Какаева приняло участие более 20 команд, состоящих из школьников и студентов средне-специальных и высших учебных заведений. В каждой команде участвовало от одного до 5 человек. В общей сложности приняло участие около 100 человек.

Был создан организационный комитет, команда жюри, положение о проведении данного мероприятия.

Для эффективного, а самое главное интересного проведения состязания было разработано два программных обеспечения, запатентованных Государственной службой Туркменистана по интеллектуальной сосбственности.

Задача первой программы автоматическое создание на компьютерах симуляций активных многоволновых угроз, искуссно замаскированных и скрытых в операционной системе.

Рис. 1 - Рабочие моменты из хакатона Turkmen Cyber.Hack

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

Таким образом, каждой комманде предоставлялся один компьютер, «загруженный» пассивными и активными угрозами. Задача команд состояла 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 пришлось действовать в непростых условиях, симулятор угроз искусно раставлял ловушки, препятствовал выполнению действий по устранению угроз, через определенные промежутки времени запускал новые волны атак, призванных запутать будущих специалистов по кибербезопасности. Нужно отметить еще тот факт, что действия команд были стеснены тем обстоятельством, что им не разрешалось 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 штрафовал команды, убавляя им баллы.

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

На выполнение поставленной задачи, участникам было отведено 4 обязательных часа, в течении которых проходили волны атак и дополнительных 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 (Рис.2.)

Работа программы состоит из 4 блоков, которые схематично расположены на указанном рисунке (Рис. 2).

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). Следует отметить, что в самой программе есть и «противоядие» для указанных «неудобств» - (кнопки, расположенные ниже).

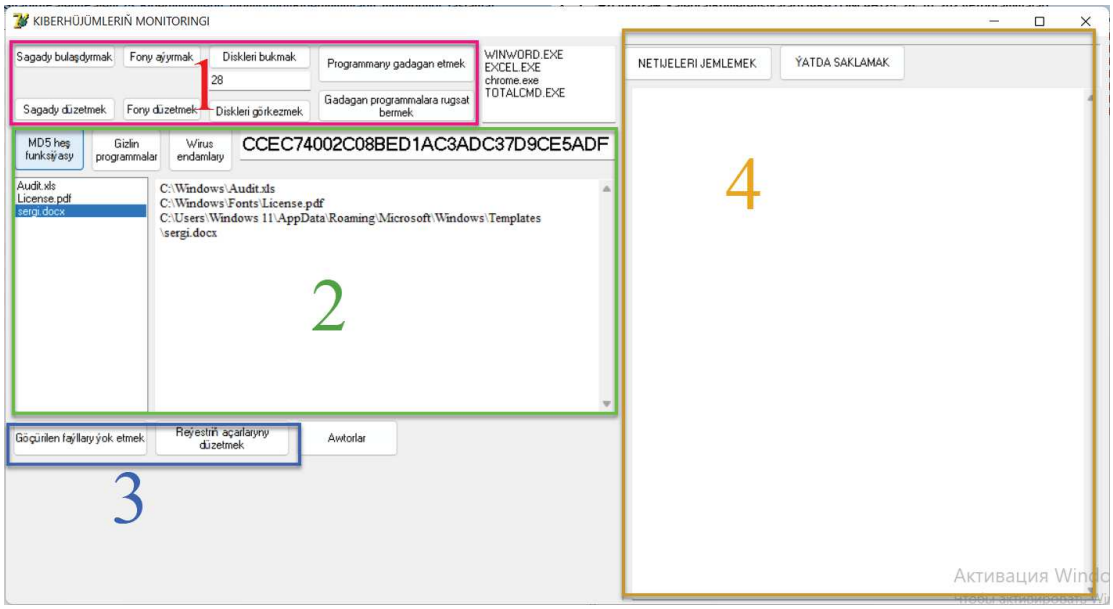

Рис. 2 - Окно программы мониторинга кибератак

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.

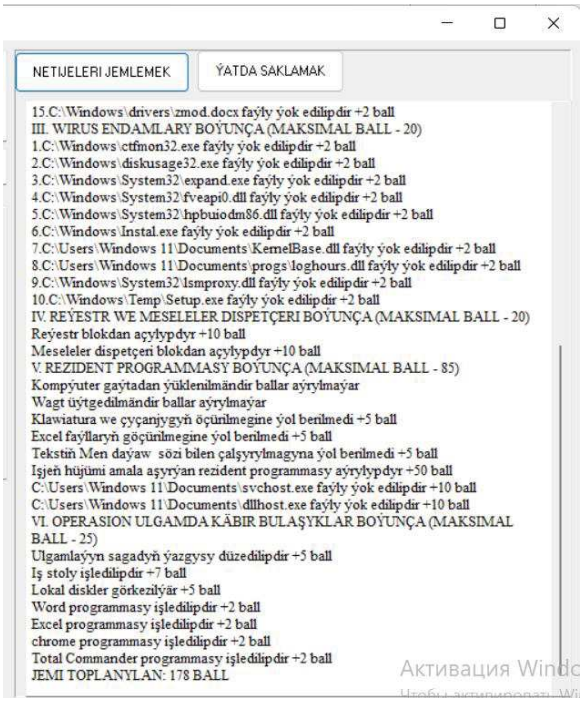

Рис. 3 - Создание отчета о состоянии системы и проделанной работе по обеспечению кибербезопасности

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.

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.

Список использованных источников

1. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум": ИНФРА - М. 2013-592с.
2. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013, 206 s.

УДК 330.16

А.Д. Чухольский, В.В. Ивановский
Белорусский государственный технологический университет
Минск, Беларусь

СТАНОВЛЕНИЕ И РАЗВИТИЕ ПОВЕДЕНЧЕСКОЙ ЭКОНОМИКИ

Аннотация. *Поведенческая экономика – это раздел экономической науки, который исследует поведение людей и его влияние на экономические решения и результаты. Поведенческая экономика основывается на исследованиях и экспериментах, чтобы понять, как мы искажаем информацию, оцениваем риски, принимаем решения при неопределенности и взаимодействуем с другими людьми.*

A.D. Chukholskiy, U.U. Ivanouski
Belarusian State Technological University
Minsk, Belarus

FORMATION AND DEVELOPMENT OF BEHAVIORAL ECONOMICS