УДК 681.3:553.98(574.4)

М.М. Чуриев[1], Б. Пирниязов[2],
А.А. Ходжагельдиев[1], У. Бердимурадова[1]
[1]Международный университет нефти и газа имени Ягшыгельди Какаева
[2]Национальный институт образования Туркменистана
Ашхабад, Туркменистан

РЕШЕНИЕ НЕКОТОРЫХ ЗАДАЧ ПО КИБЕРБЕЗОПАСНОСТИ

Аннотация. *В статье рассматриваются вопросы обеспечения кибербезопасности, проделан анализ основных причин и особенностей кибератак и кибервойн. Авторы дают описание особо важных для мониторинга ключей системного реестра. Также в работе представлено программное решение для профилактики и отражения некоторых угроз.*

M.M. Churiyev[1], B. Pirniyazov[2],
A.A. Hojageldiyev[1], U. Berdimyradova[1]
[1]Yagshigeldi Kakaev International University of Oil and Gas
[2]National Institute of Education of Turkmenistan
Ashgabat, Turkmenistan

SOLVING SOME CYBER SECURITY TASKS

Abstract. *The article deals with the issues of ensuring cybersecurity, an analysis of the main causes and features of cyber attacks and cyber wars is carried out. The authors give a description of the system registry keys that are especially important for monitoring. The paper also presents a software solution for the prevention and reflection of some threats.*

Вызовы, связанные с киберпространством и кибербезопасностью, требуют от государственных организаций, ответственных за безопасность в области информационных технологий или за безопасность в области коммуникаций решения задач защиты населения и национальных интересов от различного рода воздействий. 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.

Та сфера, которая когда-то считалась электронной войной или информационной войной, и в которой преобладали специалисты по сетевой безопасности, сегодня преобразовывается в более широкую сферу, именуемую «кибербезопасность».

Очевидно, что кибербезопасность должна быть нацелена на обеспечение защиты в киберпространстве. Кибербезопасность определяется как «деятельность или процесс, способность, возможность или состояние, при которых системы информации и связи и информация, содержащаяся в них, защищены и/или охраняются от вреда, несанкционированного использования, модификации или эксплуатации» [4].

В киберпространстве могут развиваться все более опасные и сложные угрозы. Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом, в том числе и от кибервойн [1].

Термин «кибервойны» прочно вошел не только в лексикон военных и специалистов по информационной безопасности, но и политиков, представителей экспертного сообщества. В сфере информационной безопасности термин «кибервойны» стал широко использоваться с 2007г. [2].

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: шпионаж и атаки.

Первый этап подразумевает сбор данных, посредством взлома компьютерных систем других государств.

Атаки можно разделить в зависимости от цели и задач военных действий:

- Вандализм – размещение пропагандистских или оскорбительных картинок на веб-страницах вместо исходной информации.
- Пропаганда и информационная война – использование пропаганды в контенте веб-страниц, в рассылках обращений.
- Утечки конфиденциальных данных – все, что представляет интерес, копируется со взломанных частных страниц и серверов, также секретные данные могут быть подменены.
- DDoS-атаки – атака с нескольких машин с целью нарушить функционирование сайта, системы компьютерных устройств.
- Нарушение работы компьютерной техники – атаке подвергаются компьютеры, отвечающие за функционирование оборудования военного или гражданского назначения. Атака приводит к выходу из строя техники или к ее отключению.
- Атака инфраструктурных и критически важных объектов и кибертерроризм– воздействие на машины, регулирующие инженерные,

телекоммуникационные, транспортные и другие системы, обеспечивающие жизнедеятельность населения.

Об истории кибернетических войн и об их отличительных свойствах сказано и написано немало. В данной части нашей работы мы попробуем смоделировать и спрограммировать некоторые процессы, применяемые в кибератаках, для того чтобы оценить степень угрозы, а также выработать некоторые рекомендации по их предотвращению.

Прежде всего, несомненным является высокий уровень анонимности кибератаки, который связан с трудностями определения киберагрессора. Киберагрессором может выступить любая программа. На сегодняшний день различные антивирусные программы используют хеш-функции для определения опасных программ. Однако практика показывает, что повторное компилирование программы полностью меняет ее хеш-сумму. Например, в исследованиях мы использовали обычную программу, которая запускается и отключает устройства ввода, такие, например, как мышь и клавиатура. В первоначальном состоянии ее хеш-сумма составляла 4a74f83ad1a9d1227ac4522b820132a4 (MD5). Позже ничего не меняя в программном коде она была заново откомпилирована, на этот раз ее хеш-сумма составила bc9b605bf770f6ab1e591716bda27f1b. Таким образом можно сделать вывод о несостоятельности хеш-проверки, как средства определения опасности программ, так-как одна и та же программа может иметь разные хеш-суммы.

Еще одной отличительной чертой кибератаки является неопределенность времени ее начала. Например, операционная система, отслеживает все изменения в файлах и автоматически устанавливает дату создания, открытия и редактирования файлов. Таким образом иногда удается отследить опасные файлы по времени их создания. Однако нестандартным и довольно простым способом можно обмануть систему и оставить дату создания файла без изменения. Например, рассмотрим процесс редактирования текстового файла. При его открытии (например через файловый менеджер) некоторая программа считывает дату его создания и сохраняет их в некоторых переменных (uyt_sene и uyt_wagt):

```
procedure TForm1.FileListBox1Click(Sender: TObject);
begin
memo1.Lines.LoadFromFile(FileListBox1.FileName);
uytsen(getfiledate(FileListBox1.FileName), uyt_sene, uyt_wagt);
statusBar1.SimpleText:= uyt_sene +' '+uyt_wagt;
end;
```

Далее при нажатии на кнопку сохранения, после того как система автоматически устанавливает текущую дату и время, программа вновь устанавливает дату и время файла через сохраненные переменные.

```
procedure TForm1.Button2Click(Sender: TObject);
begin
```

```
memo1.Lines.SaveToFile(FileListBox1.FileName);
SetFileDate(FileListBox1.FileName,StrToDate(uyt_sene)
+StrToTime(uyt_wagt));
end;
```

Таким образом достигается эффект неопределенности.

Следует признать и такую крайне неприятную черту кибервооружений, как чрезвычайная сложность их контроля со стороны государственных систем разведки и безопасности. Это достигается тем, что каждый потенциальный киберагрессор прекрасно осведомлен о возможностях и технологиях антивирусных и других защитных программ, так-как они могут быть установлены на его компьютере. Он может свободно проводить испытания по обходу защиты и обнаружения антивирусами на своей собственной системе и при удачных испытаниях быть уверенным в успешном осуществлении свой атаки.

Таким образом нужно разрабатывать нестандартные методы обнаружения и предупреждения, которые еще не изучены злоумышленниками.

Теперь возникает следующий вопрос - как бороться с загрузчиками и как правильно определять записи автозагрузок. Следует осуществлять мониторинг реестра - сверку записей автозагрузок с заблаговременно сохраненным списком-эталоном, следить за появлением новых строковых параметров, их соответствию заданиям системы. Осуществить это, применив функции программного оперирования реестром, не сложно.

В последнее время стали появляться загрузчики-фантомы. Обнаружить их достаточно сложно. Их автозагрузка осуществляется по следующему принципу: загрузчик запускается считыванием записи реестра, затем он удаляет эту запись, а в момент закрытия операционной системы он автоматически восстанавливает ее. И это все повторяется снова и снова …

В результате исследования над этими загрузчиками, удалось определить моменты удаления и восстановления записи реестра об их автозагрузке, а также создать программные коды, предотвращающие их загрузку. Для этого процесс сверки реестра нужно запустить после процесса восстановления записи реестра загрузчиком - это можно осуществить, перехватив сообщение операционной системы о своем завершении. Практически нужно действовать по тому же принципу что и загрузчики вирусов [3].

В данной работе мы решились взяться за одну из самых больших проблем обеспечения кибербезопасности – это своевременное обнаружение начавшейся и пока не разросшейся кибератаки. Для этого на объектно-ориентированном языке программирования было разработано специальное программное обеспечение, содержащее в своем алгоритмическом арсенале достаточно мощный механизм по обеспечению слаженной работы операционной системы и перехвату «аномальных» явлений.

Разработанное программное обеспечение позволяет решить многие вышеуказанные трудности и осуществлять контроль за выполняемой на компьютере работе и в случае необходимости обладает достаточными средствами и модулями для соответствующей защиты:

- Отображение списка запущенных программ, с возможностью завершения любой выбранной программы или создания списка завершаемых программ (против атак несколькими программами).
- Чтение в альтернативном режиме системного реестра и настройка списка программ, запускаемых вместе с системой. С помощью данного модуля можно определить какие программы, запускаются автоматически без участия пользователя.
- Запуск утилиты для ограничения или разрешения запуска указанных программ. Данный модуль программы позволяет установить и редактировать список программ, запрещенных к запуску в системе. Также есть возможность отладки запуска реестра системы, блокированного системой.
- Защита носителем флэш экрана компьютера и возможности входа в систему. Данная возможность позволяет защитить экран, специальной заставкой с паролем на флешку, при извлечении которой из компьютера, экран автоматически блокируется и только вставка именно данной флешки вновь открывает экран.
- Создание виртуальных дисков на носителях информации с возможностью сохранения в них необходимой информации защитой паролем и шифрованием. Данный модуль запускает утилиту создания специального виртуального диска с помощью закодированного файла на носителе информации.

Перечисленные выше возможности программы, позволят успешно отражать некоторые существующие виды кибератак, обеспечить киберстабильность компьютерной системы, защитить персональные данные и обеспечить безопасный обмен информацией.

Разработанная программа может быть использована на любом государственном и частном предприятии и учреждении для самостоятельной защиты пользователем своей компьютерной системы от внешних угроз.

Список использованных источников

1. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум": ИНФРА - М. 2013-592с.
2. Karl Maria Michael de Leeuw, Jan Bergstra - The History of Information Security: A Comprehensive Handbook, Elsevier Science, 2007
3. М. Чуриев, И. Комольцев, А. Муратлыев. Использование реестра в современных методах защиты. Тезисы Международной научной

конференции «Наука, техника и инновационные технологии в счастливой эпохе могучего государства» (г. Ашхабад, 12-14 июня 2012 года).
4. Hajymuhammet Geldiyev, Maksat Churiyev, Rejep Mahmudov “Chapter 1. Issues regarding cybersecuirty in modern world”, Springer Science and Business Media LLC, 2020.

УДК 338.001.36

К.К. Шебеко[1], Д.К. Шебеко[2]
[1]Белорусский государственный технологический университет
Минск, Беларусь
[2]АО «Деловые решения и технологии»
Санкт-Петербург, Россия

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СЕТЕВАЯ ЭКОНОМИКА КАК ФАКТОР ЭКОНОМИЧЕСКОГО РАЗВИТИЯ

Аннотация. *Изложены результаты исследования взаимосвязи индекса сетевой готовности (Network Readiness Index) и уровня экономического развития стран (GDP per capita, PPP (current international $)). На основе использования предложенной модели приведены прогнозные значения ВВП на душу населения по Беларуси и соседним странам*

K.K. Shebeko[1], D.K. Shebeko[2]
[1]Belarusian State Technological University
Minsk, Belarus
[2]Business Solutions and Technologies
Saint-Petersburg, Russia

INFORMATION AND COMMUNICATION TECHNOLOGIES AND THE NETWORK ECONOMY AS A FACTOR OF ECONOMIC DEVELOPMENT

Abstract. *The results of a study of the relationship between the Network Readiness Index and the level of economic development of countries (GDP per capita, PPP (current international $)) are presented. Based on the use of the proposed model, forecast values of GDP per capita for Belarus and neighboring countries are calculated.*

Количественная оценка влияния различных факторов на развитие национальных экономик всегда вызывает интерес в деловых, научных