углубления образовательного процесса Союзного государства. Реализация совместной образовательной программы будет способствовать подготовке компетентных специалистов в сфере международного экономического сотрудничества на постсоветском пространстве и развитию единого образовательного пространства Союзного государства.

Список использованных источников

1. Договор о создании Союзного государства [Электронный ресурс]: [подписан 08.12.1999]// КонсультантПлюс: Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.
2. Выяснилось, сколько белорусов учится в России в 2023 году [Электронный ресурс]. – Режим доступа: https://sputnik.by/20230220/vyyasnilos-skolko-belorusov-uchitsya-v-rossii-v-2023-godu-1072459523.html. – Дата доступа: 10.11.2023.
3. Тарарышкина, Л.И. Дистанционное образование: драйвер экономического роста государств-членов Евразийского экономического союза /О.В. Жданович, Л.И. Тарарышкина//Интеграционные процессы в Евразии: состояние, вызовы, перспективы: сборник научных статей I Международной научно-практической конференции (Республика Беларусь, Минск, 17 февраля 2023 г.)/ Белорусский государственный университет; редкол.: ЕА.Достанко (гл. ред.) [и др.]. – Минск:Четыре четверти, 2023. – С.141-145.

УДК 681.3:553.98(574.4)

А.А. Тячмухаммедов[1], А.Р. Доглотов[1], М.Р. Отузов[1], Дж.Ч. Чуриев[2]
[1]Международный университет нефти и газа имени Ягшыгельди Какаева
[2]Институт инженерно-технических и транспортных коммуникаций Туркменистана
Ашхабад, Туркменистан

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ ПРОТИВ ТРОЯНСКИХ АТАК

Аннотация. *В статье рассматривается проблема разработки и применения программного обеспечения «Антитроян». «Антитроян» создавался в экспериментальных условиях - на экспериментальном компьютере запускались самые злостные вирусы, далее разрабатывались методы по их ручному удалению. Эти методы программировались и компиллировались в машинный код. Таким образом было разработано «боеспособное» программное обеспечение по своевременному выявлению и противодействию троянской угрозе.*

A.A. Tachmuhammedov[1], A.R. Doglotov[1], M.R. Otuzov[1], J.Ch. Churiyev[2]
[1]Yagshigeldi Kakaev International University of Oil and Gas
[2]Institute of Engineering - Technical and Transport Communications of Turkmenistan
Ashgabat, Turkmenistan

DEVELOPMENT OF SOFTWARE TOOLS AGAINST TROJAN ATTACKS

Abstract. *The article examines the problem of developing and using Antitrojan software. "Antitrojan" was created under experimental conditions - the most malicious viruses were launched on an experimental computer, and then methods were developed to manually remove them. These methods were programmed and compiled into machine code. Thus, "combat-ready" software was developed to timely identify and counter the Trojan threat.*

Мировая практика показывает важность решения вопросов информационной безопасности для обеспечения национальной безопасности. Ни одна страна в мире не является защищенной от основных видов киберпреступности, которыми являются компьютерные вирусы, хакерские атаки, спам рассылки и другие мошеннические схемы в Интернете.

Вопросы связанные с киберпространством и кибербезопасностью требуют от организаций в сфере информационных технологий, коммуникаций и ответственных за безопасность государственных структур обеспечения безопасности населения от цифровых опасностей и решения вопросов национальной безопасности.

Повсеместное использование компьютерных систем и распространение разных устройств от мобильных телефонов до переносных компьютеров обусловило появление уязвимостей и всевозможных векторов опасности в цифровой среде для государственных и негосударственных предприятий.

Эксплуатация таких уязвимостей, шпионаж, падение эффективности распорядительных и управленческих объектов, кража

интеллектуальной собственности и чувствительных данных личного характера, нарушение деятельности важных инфраструктур и систем обслуживания, намеренное нанесение вреда экономике и промышленности могут крайне отрицательно повлиять на национальную безопасность [1].

Кибербезопасность определяется как процесс, умение, возможность или работа информационных систем, систем связи и данных содержащихся в этих системах в защищённом или защищаемом от несанкционированного доступа, редактирования или эксплуатирования порядке. Самыми опасными явлениями в киберпространстве являются кибервойны.

Кибервойна – это деятельность направленная на разрушение материальных объектов информационных потоков и их систем, нарушение их работоспособности и захват управления информационными системами противника. Основные деловые и финансовые центры, государственные предприятия теряют свою работоспособность в результате кибервойн. Также кибервойны приводят к беспорядкам в общественной жизни.

В следствии этих происшествий происходят сбои в работе важных инфраструктурных и функциональных систем. К таким системам относятся система канализации, электрические станции, энергетические узлы и другие коммуникационные сети. Главным средством ведения войны в киберпространстве является программный код, который обеспечивает нарушение работоспособности объектов или позволяет взять под контроль управление материальных объектов оборудованных электронными системами управления и систем управления сетей [2].

Изучая и анализируя разного рода опасности и атаки было выявлено, что большинство из них использует реестр операционной системы. Реестр – это средство управления и настройки операционной системы [3]. Ключи автозагрузки, которые входят в состав реестра позволяет запускать систему и его составные элементы, и пользовательские программы. Вместе с этими программами могут загружаться и шпионские или более опасные вирусы и программы. Пользователь может и не догадываться о существовании таких процессов.

Было проведено немало работы по анализу специальных ключей реестра. По результатам этих работ были разработаны алгоритмы по выявлению шпионских программ, троянских вирусов и других вредоносных программ.

Специальное антивирусное программное обеспечение, названное «Антитрояном» и нацеленное на выявление и устранение вредоносных программ было разработано преподавателями и студентами университета при приминении таких алгоритмов. Для этой программы было получено свидетельство №36 (патент) от соответствующих организаций.

Теперь рассмотрим технические особенности программы «Антитроян»:

1. Скорость работы программы. Под скоростью работы антивируса подразумевается скорость проверки разделов операционной системы (файлы и папки) в определенный промежуток времени. То есть, программа проверяет 200 мегабайт данных за одну секунду. Эта скорость позволяет полностью проверить современный компьютер за 40-50 минут.

2. Вирусная база программы. Под вирусной базой программы подразумевается количество вирусов, которые антивирус может выявить и полностью устранить. Программа способна выявить и удалить около 300 вирусов и вредоносных программ. Большинство широко распространенных антивирусов не способны выявлять около 20% из этих 300 вирусов.

3. Совместимость с операционной системой. Разработанный антивирус способен работать на разных операционных системах семейства Microsoft, таких как XP, Vista, Windows 7, 8 и 10. А 99% компьютеров в Туркменистане работают именно на этих системах.

4. Совместимость с другими программами. Под этим подразумевается работа с другими программами. Антивирус может быть установлен на компьютер с вирусом и устранить вредоносные программы без каких-либо проблем, спокойно работает в координации с другими антивирусами и не создают препятствий для устойчивой работы других пользовательских программ.

5. Срок работы программы. Срок работы программы - это время с которого программное обеспечение было установлено и начало работу на компьютере. Срок работы программы неограничен.

6. Заражение программы. Заражение программы – это заражение программы вирусом или вредоносной программой. Программа, имеет возможность вести мониторинг и удалиться с компьютера при заражении вирусом.

7. Интерфейс программы. Интерфейс программы – это визуальные возможности, которые программа может предложить пользователю. Программа работает с двумя языками интерфейса –

русский и туркменский. Также этот антивирус обеспечен справочником и возможностями поиска.

8. Дополнительные возможности. При выявлении разных уязвимостей в операционной системе компьютера, можно использовать разделы самостоятельной работы процессов и реестра.

9. Размер программы. «Антитроян» занимает примерно 2 мегабайта в памяти компьютера.

Некоторые кибератаки невозможно выявить или выследить посредством антивирусных программ, так как они могут работать долгое время не причиняя никакого вреда операционной системе или компьютеру в целом. Таким образом, они имеют свойство анонимного режима работы. После определенного времени эти программы всё-таки начинают свою шпионскую или другую вредоносную деятельность. Например, они могут после определенного срока, указанного в их настройках, скрыто копировать данные компьютера на съёмный носитель информации.

Анализируя работу подобных программ, было разработано другое программное обеспечение. Описываемое программное обеспечение нацелено на решение этих проблем, контроль работы компьютера и, при необходимости, предлагает необходимые средства для обеспечения безопасности:

- показать список активных программ компьютера и при необходимости закрыть эту программу;
- чтение системного реестра в автономном от системы режиме и настройка списка автоматически запускающихся вместе с системой программ;
- разрешение указанным программам запуска в системе и запуск утилиты для введения запрета;
- защита экрана и возможности входа в систему с помощью флеш-памяти;
- создание виртуальных дисков, и хранение в них защищенных паролем данных, шифровка этих данных.

Описанные выше возможности позволяют бороться против определённых видов кибератак и обеспечивать кибербезопасность компьютеров и операционных систем.

Разработанное программное обеспечение может быть установлено и использоваться в любом предприятии на любом компьютере с операционной системой Windows. Составные части и компоненты множества вредоносных программ были изучены научной командой Международного университета нефти и газа имени Ягшыгелди Какаева. Члены этой группы занимаются вышеописанными

проблемами. Кроме того, разрабатываются программные средства, нацеленные на решение вопросов кибербезопасности электронной системы обучения университета.

Обеспечение информационной безопасности невозможно без выполнения следующих действий:

- обеспечение защиты от несанкционированного доступа;
- обеспечение защиты интеллектуальной собственности;
- предотвращение распространения в Интернете компьютерных вирусов, спама и шантажа;
- развитие национальной законодательной базы определения порядки применения специальных средства защиты в Интернет среде;
- разработка регулирующих условий для выявления и наказания злоумышленников;
- подготовка кадров, способных бороться с самыми опасными угрозами в цифровой среде.

Выполнение этих работ поможет решить проблему обеспечения безопасности Цифровой системы образования.

Список использованных источников

4. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум": ИНФРА - М. 2013-592с.

5. Karl Maria Michael de Leeuw, Jan Bergstra - The History of Information Security: A Comprehensive Handbook, Elsevier Science, 2007.

6. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013, 206 s.

УДК 003.26

Н.И. Уласевич
Белорусский государственный технологический университет
Минск, Беларусь

СТЕГАНОГРАФИЧЕСКИЕ РЕШЕНИЯ В SVG ФАЙЛАХ

Аннотация. *В рамках статьи изучаются и анализируются методы и алгоритмы встраивания информация в векторных файлах. Рассмотрены некоторые особенности отображения и стеганографии в векторных файлах.*