РОССИЙСКАЯ ФЕДЕРАЦИЯ

Ханты-Мансийский автономный округ - Югра (Тюменская область)

город Нижневартовск

Тема: «Вирусы – угроза современным гаджетам».

Автор: Гаренских Даниил Вячеславович, 7 «А» класс.
Муниципальное бюджетное общеобразовательное учреждение «Средняя школа №25».

Руководители: Бирлова Татьяна Леонтьевна,
учитель информатики.
Муниципальное бюджетное общеобразовательное учреждение «Средняя школа №25».

2017г.

Тема: «Вирусы – угроза современным гаджетам»

Гаренских Даниил Вячеславович, Муниципальное бюджетное общеобразовательное учреждение «Средняя школа №25», 7 «А» класс

АННОТАЦИЯ

Современный человек без новомодных гаджетов уже не представляет свою жизнь и чем больше они проникают в нашу жизнь, тем большему риску подвергаемся мы со стороны хакерских атак и атак вредоносных программных продуктов, в результате которых человечество несет огромные финансовые убытки. Не стоит забывать, что нынешний смартфон, это уже не вчерашний «кнопочный телефон», это современный мини компьютер, управляемый операционной системой на всемирно известных платформах Apple iOS, Google Android, Windows Phone, Symbian, Blackberry OS.

По данным статистических исследований за последний год, взятых с сайта AZERICMS очевидно, что Android бьет по популярности все другие операционные системы, даже такие операционные системы, как IOS и Symbian, которые когда-то были лидерами отрасли, остались далеко позади (приложение I, фото 1).

И как следствие этому особый интерес для киберпреступников представляет именно та операционная система, которая пользуется максимальным спросом - Android. Для данной платформы пишется около 96 % от всех существующих образцов вредоносного программного обеспечения для мобильных устройств.

Вероятность заражения современных гаджетов вирусами особенно велика тогда, когда мы выполняем самые распространенные действия - устанавливаем на свое устройство различные приложения или посещаем сомнительные сайты, при этом на экране может появиться соответствующее уведомление (приложение I, фото 2).

В связи с этим, тема вирусов, заражающих наши гаджеты, является актуальной.

Цель выяснить, какой гаджет наиболее популярен в настоящее время, действительно ли существует проблема заражения вирусами современных гаджетов.

Задачи 1. Изучить литературу и Интернет-ресурсы по данной проблеме. 2. Провести социологическое исследование, выявить проблему, если она есть у исследуемых, предложить свой вариант её решения.

Методы исследования. Теоретические – анализ источников, систематизация и обобщение информации. Эмпирические – эксперимент, опрос, наблюдение, диагностика, сравнительный анализ.

Тема: «Вирусы – угроза современным гаджетам»

Гаренских Даниил Вячеславович, Муниципальное бюджетное общеобразовательное учреждение «Средняя школа №25», 7 «А» класс

План исследования

В настоящее время наблюдается стремительный рост развития информационной сферы в жизни современного общества и поэтому проблема защиты информации очень актуальна проблема защиты любой, важной для человечества, информации становиться все более актуальной. Информация приобрела статус потребительского продукта, потому что стала востребована на рынке товаров и услуг и стала приносить прибыл. А если информация приносит высокую прибыль, значит, она имеет ценность и тут возникает проблема, связанная с ее защитой. Говоря о защите информации, следует акцентировать свое внимание на следующие аспекты, потеря ее ценности, либо ее исчезновение с устройств хранения данных. Первый аспект связан с человеческим фактором, а второй с технической стороной. К человеческим факторам, прежде всего можно отнести халатность владельцев той или иной информации, а техническая сторона предполагает возможность сбоев в работе аппаратной части устройств, на которых хранится информация или же из-за вирусов, проникших в те или иные устройства. В данной работе мы хотим рассмотреть различные угрозы для мобильных устройств и выделить более эффективные способы защиты от них.

Современный человек без новомодных гаджетов уже не представляет свою жизнь и чем больше они проникают в нашу жизнь, тем большему риску подвергаемся мы со стороны хакерских атак и атак вредоносных программных продуктов, в результате которых человечество несет огромные финансовые убытки. Не стоит забывать, что нынешний смартфон, это уже не вчерашний «кнопочный телефон», это современный мини компьютер, управляемый операционной системой на всемирно известных платформах Apple iOS, Google Android, Windows Phone, Symbian, Blackberry OS.

По данным статистических исследований за последний год, взятых с сайта AZERICMS очевидно, что Android бьет по популярности все другие операционные системы, даже такие операционные системы, как IOS и Symbian, которые когда-то были лидерами отрасли, остались далеко позади (приложение I, фото 1).

И как следствие этому особый интерес для киберпреступников представляет именно та операционная система, которая пользуется максимальным спросом - Android. Для данной платформы пишется около 96 % от всех существующих образцов вредоносного программного обеспечения для мобильных устройств.

Вероятность заражения современных гаджетов вирусами особенно велика тогда, когда мы выполняем самые распространенные действия - устанавливаем на свое устройство различные приложения или посещаем сомнительные сайты, при этом на экране может появиться соответствующее уведомление (приложение I, фото 2).

В связи с этим, тема вирусов, заражающих наши гаджеты, является актуальной.

Объект исследования: мобильный вирусы.

Проблемный вопрос: действительно ли вирусы являются угрозой современных гаджетов, если да, то как защитить свое устройство от них?

Актуальность темы: в том, чтобы суметь распознать вирус, и научиться защищать свой гаджет.

При изучении этой темы были поставлены следующие цели и задачи.

Цель исследования: Выяснить, какой гаджет наиболее популярен в настоящее время, действительно ли существует проблема заражения вирусами современных гаджетов.

Задачи исследования: изучить литературу и Интернет-ресурсы по данной проблеме, провести социологическое исследование, выявить проблему, если она есть у исследуемых, предложить свой вариант её решения.

Гипотеза: если вирусы существуют, то действительно ли они могут нанести вред современным гаджетам.

Методы исследования. Теоретические – анализ источников, систематизация и обобщение информации. Эмпирические – эксперимент, опрос, наблюдение, диагностика, сравнительный анализ.

Объект: обучающиеся 5-11 классов и педагогические работники МБОУ «СШ №25» (109 респондентов).

План исследовательской работы:

Октябрь-ноябрь 2016г. – выбор темы исследования, постановка цели, задач. Сбор информации.

Декабрь 2016г. – январь 2017г. – проведение социологического исследования, эксперимент, съёмки видеоролика.

Февраль 2017г. – оформление исследовательской работы, подготовка презентации.

Библиография: 1. Создаем вирус и антивирус. Автор: И.А. Гульев, 304с. – М.: Просвещение, 1999г. 2.Защита от мобильных вирусов [Электронный ресурс] — Режим доступа. — URL: http://www.utro.ru/articles/ 2013/10/29/1153228.shtml. 3. Все о мобильных телефонах: Возможности, выбор, этикет. Автор: Инджиев А.А. – М.: Феникс, 2006г.

Тема: «Вирусы – угроза современным гаджетам»

Содержание

Тема: «Вирусы – угроза современным гаджетам»

Гаренских Даниил Вячеславович, Муниципальное бюджетное общеобразовательное учреждение «Средняя школа №25», 7 «А» класс

Научная статья

«Думаю, компьютерные вирусы можно считать
новой формой жизни. И это, пожалуй, кое-что говорит
о природе человека, коль скоро единственная форма жизни,
которую нам удалось создать, — чисто разрушительная.
Мы сотворили жизнь по своему образу и подобию».
Стивен Хокинг.

Введение

Мобильные вирусы – это небольшие программы, предназначенные для вмешательства в работу мобильного телефона, смартфона, коммуникатора, которые записывают, повреждают или удаляют данные и распространяются на другие устройства через сообщения, во время загрузки и установки различных приложений и во время путешествия по всемирной компьютерной сети Интернет.(1)

Основная часть

1. Теоретическая часть

1.1 Разновидности угроз и от чего необходимо защищать информацию.

Компьютерные преступления условно можно подразделить на две большие категории: преступления, связанные с вмешательством в работу компьютеров и преступления, использующие компьютеры, как необходимые технические средства. Перечислю некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров.

Компьютерные преступления

1) ***Несанкционированный доступ к информации***, хранящейся в компьютере. Его осуществляют хакеры.Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами идентификации, например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.д., оказываются без защиты против этого приема.

2) ***Ввод в программное обеспечение «логических бомб»***, которые срабатывают при выполнении определенных условий и частично или полностью разрушают компьютерную систему. С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

3) Разработка и распространение компьютерных вирусов. Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению. В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру, начиная от безобидных шуток заканчивая действиями, ведущими к потере информации и полной остановке работы компьютера» [9].

4) Подделка компьютерной информации. Этот вид компьютерной преступности является одним из наиболее «свежих». К подделке информации можно отнести, например подтасовку результатов выборов, голосований и т.д. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

5) Хищение компьютерной информации. Если «обычные» хищения попадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. «Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования зачастую не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации» [11]. Поэтому пиратство тоже можно отнести к хищению.

Все эти преступления попадают под различные статьи УК РФ, хотя за частую доказать факт преступления очень сложно.[8]

1.2. Что такое вирусы? Почему их надо бояться?.

Не смотря на то, что не имеется научного определения понятия «Компьютерный вирус», но его можно охарактеризовать так - «Компьютерный вирус» - это программа, которая может копировать себя в другие программы, чтобы продолжать размножение, выполняясь вместе с ними, и возможно, совершать некоторые побочные действия от безобидных шуток до действий, ведущих к потере информации и полной остановке работы компьютера [9].

Авторами вирусов могут быть профессиональные программисты, студенты и даже дети школьного возраста. Написать работающий вирус не составляет большого труда.

Классификация вирусов.[1]

- **Вирусы-спутники** - не изменяют файлы. Алгоритм работы этих вирусов таков: они создают для EXE файлов файлы-спутники, имеющие такое же имя, но с расширением COM. Вирус записывается в COM файл и никак не изменяет EXE файл. При запуске такого файла DOS первым обнаружит и выполнит COM файл то есть вирус, который затем запустит и EXE файл.

[1] Лаборатория Касперского. Классификация компьютерных вирусов. [Электронный ресурс]// Интернет-журнал «Энциклопедия необходимых компьютерных знаний». - 2012. – 8 января. Адрес: http: http://www.ezpc.ru/pcvir2.shtml

- **Вирусы-черви** - вирусы, которые распространяются в компьютерной сети и, они так же не изменяют файлы. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.
- **Паразитические** - все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу попадают все вирусы, которые не являются червями или спутниками.
- **Студенческие** - крайне примитивные, часто не резидентные и содержащие большое число ошибок.
- **Стелс-вирусы (вирусы-невидимки)**, представляющие собой «серьёзные» программы, которые перехватывают обращения ДОС к зараженным файлам или к секторам и подставляют вместо себя не зараженные участки информации.
- **Вирусы-призраки (полиморфные)** - достаточно трудно обнаруживаемые вирусы, не имеющие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса-призрака не будут иметь ни одного совпадения.

В настоящий момент не существует лучшего метода борьбы с ними, чем регулярно обновление антивирусной программы.

1.3. Классификация антивирусных программ.

Существуют следующие виды антивирусных программ:программы-детекторы;

- программы-доктора;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины.

Программы-детекторы осуществляют поиск характерных для конкретного вируса признаков в оперативной памяти и файлах, при обнаружении они выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только известные разработчикам вирусы.

Программы-доктора, или фаги, а также программы-вакцины не только находят зараженные файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в рабочее состояние. Наиболее известные из них: Kaspersky Antivirus, Norton AntiVirus, Doctor Web. В связи с тем, что постоянно появляются новые вирусы, программы-детекторы и программы-фаги быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры являются самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сра-

зу после загрузки операционной системы. К числу программ-ревизоров относится широко распространенная программа Kaspersky Monitor.

Программы-фильтры или «сторожа» представляют собой небольшие программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться: попытки коррекции файлов с расширениями COM. EXE; изменение атрибутов файла.

При попытке какой-либо программы произвести эти действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на ранней стадии его существования, до размножения. Однако они не «лечат». Для уничтожения вирусов требуется применить другие программы - фаги.

Вакцины – это резидентные[2] программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Эти программы защищают только от известных вирусов. Вакцина изменяет программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры

2. Практическая часть

2.1 Анкетирование учащихся

В рамках исследования нами было проведено анкетирование обучающихся 5-11 классов и педагогических работников школы города Нижневартовска.

Для этого нами была разработана анкета (приложение II). В анкетирование приняли участие 109 человек: 23 педагога и 86 обучающихся.

Результаты проведенного социологического опроса показали, что большинство респондентов из всех современных гаджетов большее предпочтение отдают смартфонам (78%), а так же опрашиваемые знают о том что такое вирусы (100%). 50% опрошенных знают как защитить свое устройство и информацию, которая в нем хранится. Большинство (70%) опрошенных никогда не сталкивалось с вирусами для мобильных устройств, 53% ответили, что не знают людей у которых, были проблемы с гаджетами из-за вирусов. 95% отметили, что задумались о проблеме вирусов для современных устройств.

[2] Означает «невидимый», «фоновый».

Анализ проведённого опроса позволяет согласиться с утверждением, что вирусы существуют и могут причинить вред нашим гаджетам.

Заключение

Данная работа посвящена очень важной проблеме современности - проблеме защиты современных устройств от вредоносных программ, хакерских атак и т.п. В наше время люди всё больше и больше занимаются поиском путей решения данной проблемы, но, не смотря на это, всегда найдётся немало прорех или способы её обойти. Список преступлений в этой области достаточно широк и очень разнообразен. Наиболее популярными из них являются: несанкционированный доступ к информации, ввод в программное обеспечение «логических бомб», разработка и распространение вирусов, хищение информации и персональных данных пользователей. Все эти преступления попадают под различные статьи УК РФ, но доказать факт преступления очень сложно.

Результаты нашего исследования показали, что почти 100% респондентов осознают важность использования антивирусного программного обеспеченья.

По результатам нашего тестирования выяснилось, что проблема защиты от вирусов остается актуальной и до конца не решенной.

Таким образом, наша гипотеза, заключающаяся в том, что информацию на компьютере нужно защищать не только от вирусов, но и от несанкционированного доступа, кражи и использования информации против её обладателя - подтвердилась.

Полученные результаты исследования дают возможность утверждать, что продукт (информационный буклет) исследовательской работы, является актуальным и востребованным. Материалы работы могут быть использованы широким кругом заинтересованных лиц, для обеспеченья безопасности обрабатываемой информации.

ЛИТЕРАТУРА

1. Бармен, Скотт. Разработка правил информационной безопасности. - М.: Вильямс, 2002. - 208 с.

2. Галатенко, В. А. Стандарты информационной безопасности. - М.: Интернет-университет информационных технологий, 2006. - 264 с.

3. Галицкий, А. В.Защита информации в сети - анализ технологий и синтез решений/ А. В. Галицкий, С.Д. Рябко.- М.: ДМК Пресс, 2004. - 616 с.

4. Лепехин, А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. - М.: Тесей, 2008. - 176 с.

5. Лопатин, В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. - М.: 2000. - 428 с.

6. Петренко, С. А. Управление информационными рисками. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.

7. Петренко, С. А. Политики информационной безопасности/ С. А. Петренко, В. А. Курбатов. - М.: Компания АйТи, 2006. - 400 с.

8. Статьи 272 УК , 274 УК РФ

9. Сайт лаборатории Касперского. Кто и почему создает вредоносные программы? [Электронный ресурс]// Детектируемые объекты. Адрес: http://www.securelist.com/ru/threats/detect?chapter=33.

10. Сайт лаборатории Касперского. Классификация детектируемых объектов // Детектируемые объекты. Адрес: http://www.securelist.com/ru/threats/detect?chapter=329.

11. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с.

12. Компьютерная безопасность: вопросы и решения. Адрес: http://comp-bez.ru/?p=164

Приложения **I**

Фото 1

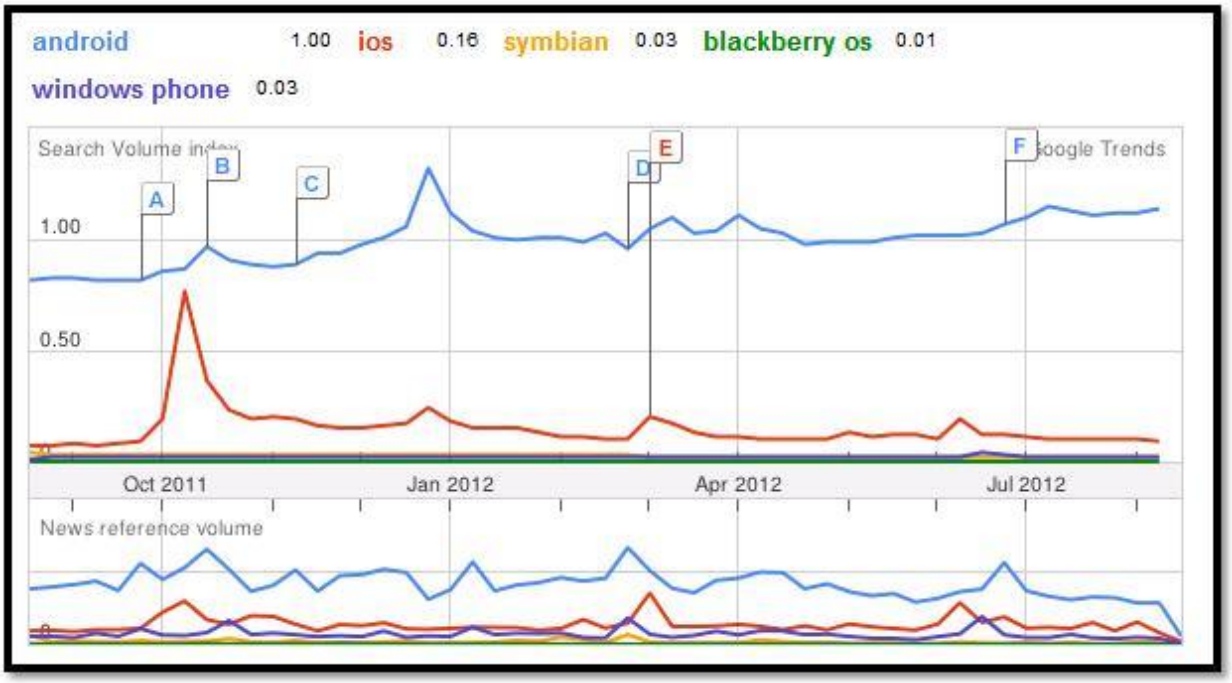
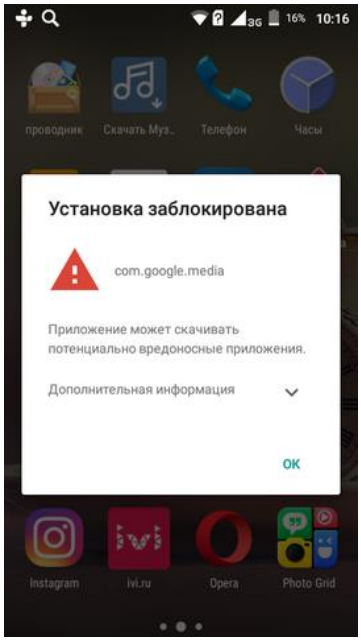


Фото 2



Приложения

АНКЕТА

«Вирусы – угроза современным гаджетам».

1. Ваш статус:
   - Обучающийся
   - Педагогический работник
2. Какой современный гаджет вы чаще всего используете для выхода в глобальную компьютерную сеть Интернет?
   - Смартфон
   - Планшет
   - Персональный компьютер
   - Другое
3. Знаете ли вы о том, что такое компьютерный вирус?
   - Да
   - Нет
4. Знаете ли вы о том, что такое мобильный вирус?
   - Да
   - Нет
5. Подвергались ли Вы риску заражения вирусом вашего мобильного устройства?
   - Да
   - Нет
6. Знаете ли Вы о том, как вирус проникает в ваше мобильное устройство?
   - Да
   - Нет
7. Знаете ли Вы что-нибудь о мобильных антивирусных программах?
   - Да
   - Нет
8. Установлена ли на вашем гаджете антивирусная программа?
   - Да
   - Нет
9. Как вы думаете, антивирусные программы эффективны в борьбе с мобильными вирусами?
   - Да
   - Нет
10. Как вы защищаете свой гаджет от вирусов?
    - _____