г.Рубцовск
2015г.

Цель:

Выяснить, существует ли проблема вирусов для мобильных телефонов и как относятся к этой проблеме владельцы сотовых телефонов.

Задачи:

- ✔ Провести анализ литературы, для изучения проблемы мобильных вирусов.
- ✔ Выяснить, что такое мобильные вирусы?
- ✔ Есть ли реальная опасность подхватить мобильные вирусы на свой мобильный телефон?
- ✔ Какое мобильное устройство больше подвержено угрозе мобильных вирусов: мобильный телефон, смартфон или только КПК?
- ✔ Что делать, если ваш телефон "заболел" (подхватил мобильный

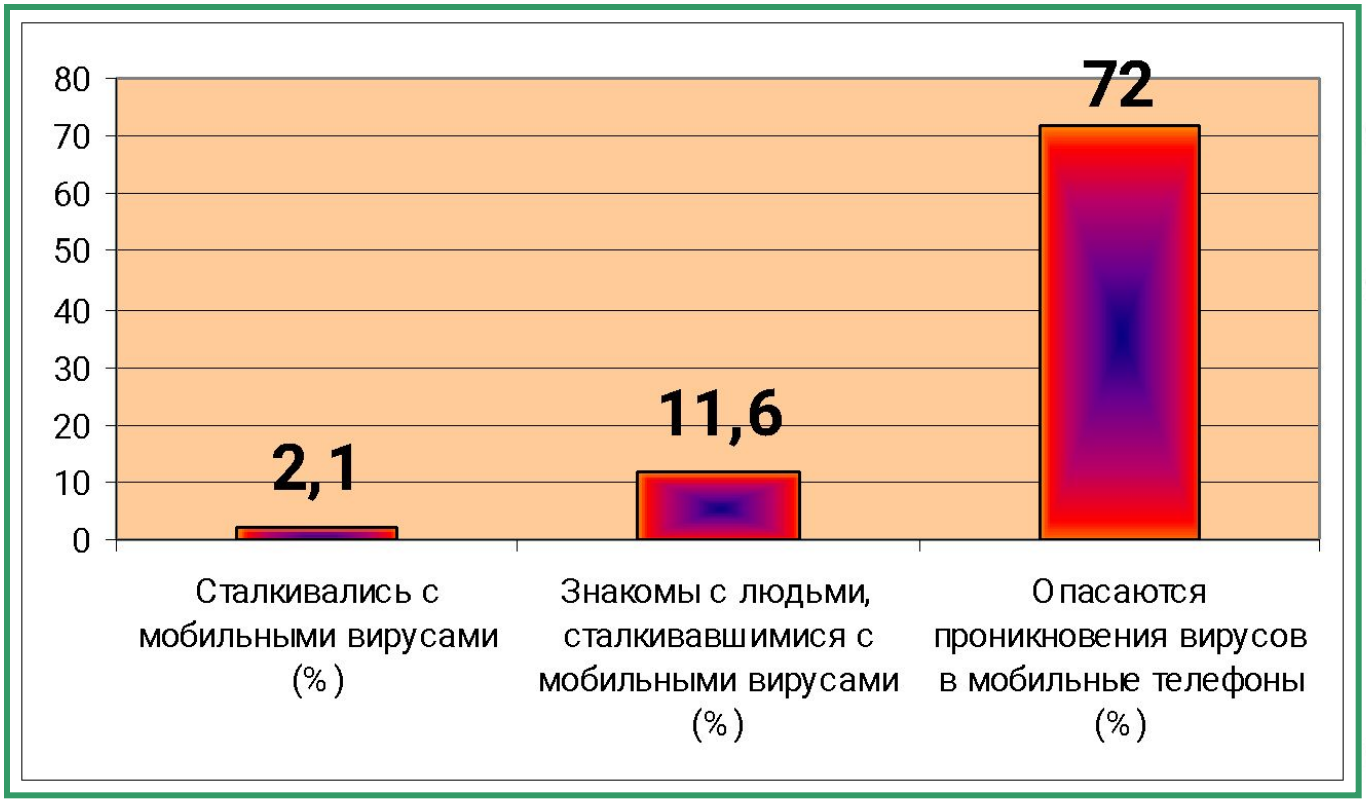
Практическое применение:

заключается в том, чтобы помочь учащимся научиться различать мобильные вирусы, защищаться от заражения телефона.

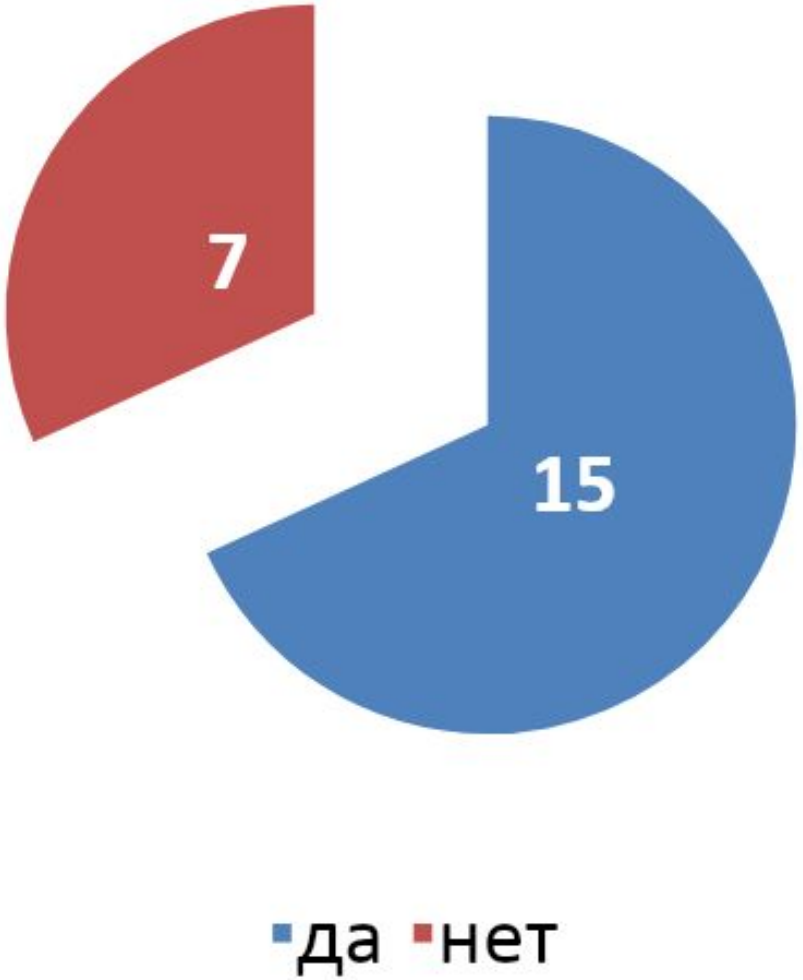
Гипотеза:

Можно предположить, что мобильные вирусы существуют, и они могут повлиять на работоспособность мобильных телефонов.

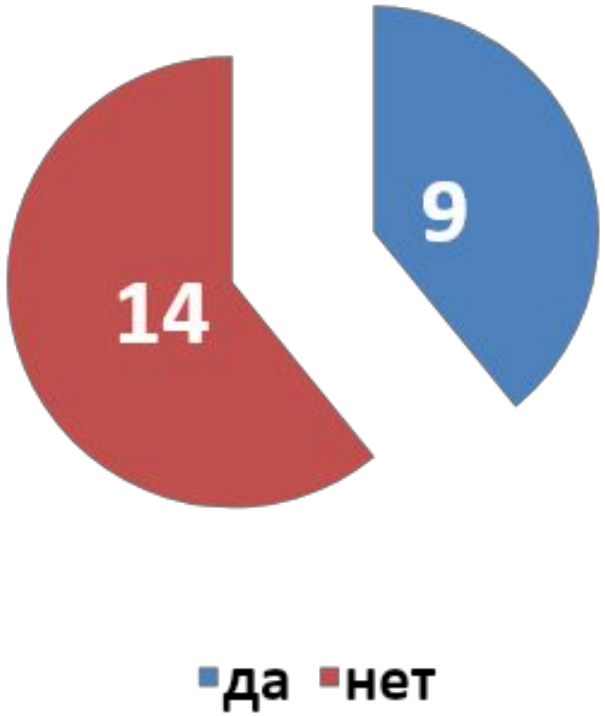
Результаты опроса проведенного антивирусной компанией McAfee среди 2000 жителей Великобритании, Соединенных Штатов и Японии.



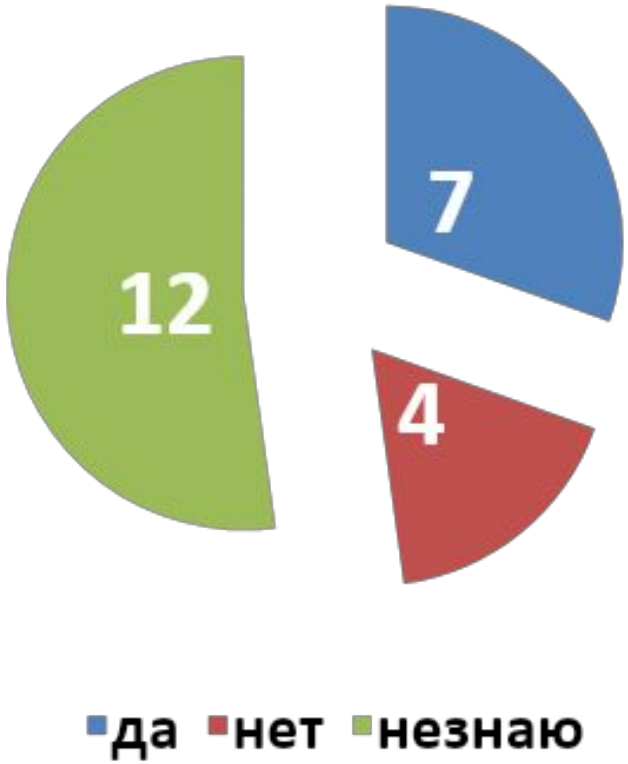
1. Слышали ли вы о мобильных вирусах?



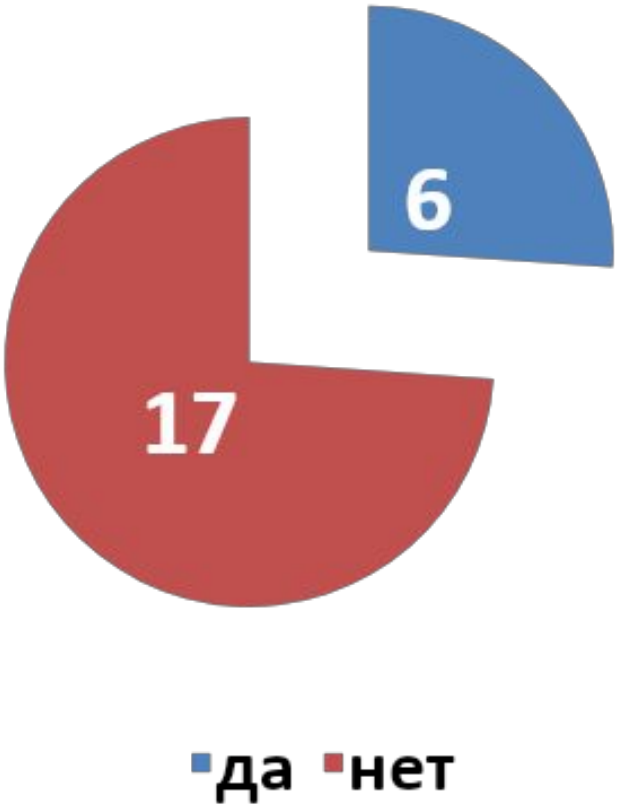
2. Знаете ли Вы каким способом мобильный вирус проникает в телефон?



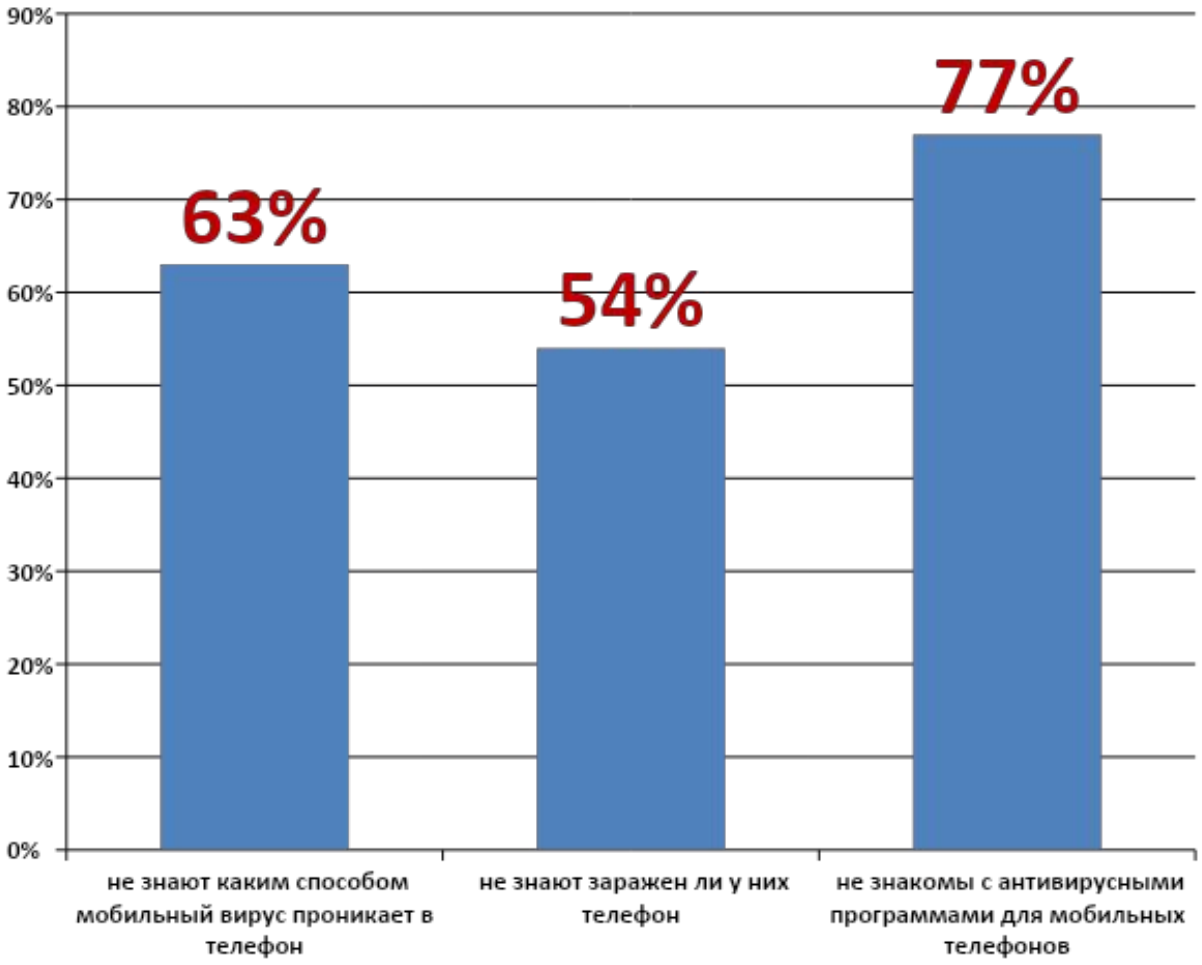
3. Было ли у Вас заражение телефона вирусом?



4. Знакомы ли Вы с антивирусными программами для мобильных телефонов?



Анкетирование показало:



История

мобильных вирусов насчитывает чуть менее десяти лет – достаточно серьезный возраст по меркам сотового рынка.

2000 год **– появление программы Timofonica.**

В июне *2004 года* группой вирусописателей 29A был разработан первый настоящий мобильный вирус – Cabir.

В феврале *2006 года* появился RedBrowser – первый мобильный вирус для телефонов с поддержкой Java.

Вирус для сотового телефона представляет собой приложение, которое маскируется под какую-нибудь игру или завлекательный интернет-файл. После того как абонент скачивает его на свой телефон, начинается «*подрывная деятельность*». Мобильный вирус может либо заблокировать карту памяти, либо незаметно для пользователя *рассылать SMS- или MMS-сообщения на платные номера*, он может также воровать данные из адресной книжки и отправлять их хозяину зловредной программы.

Червивое разнообразие

- Вирус-червь Cabir
- Вирус CommWarrior
- Вирус-Шпион Flexispy
- Кросс-платформенный вирус Cxover
- Вирус-троян RedBrowser
- Вирус-троян Webster

Вирус-червь Cabir

Первый вирус для сотовых телефонов был обнаружен в *2004 году*, и со временем под его действием оказалось 23 страны. Это так называемый компьютерный червь, получивший название **Cabir**. Он заражает смартфоны на Symbian. Вирус доставляется на трубку в виде SIS-файла, маскируясь под утилиту управления безопасностью. «Зараженный» смартфон начинает поиск других уязвимых аппаратов и пересылает на них файл, содержавший червя.

Вирус не уничтожает пользовательские данные, но блокирует санкционированные Bluetooth-соединения и потребляет ресурсы аккумулятора.

Вирус CommWarrior

В 2005 году появился более опасный вирус, чем Cabir. Его назвали *CommWarrior*. Эта программа довольно долго терроризировала смартфоны абонентов 22 стран мира. CommWarrior атаковал Symbian-аппараты на S60 и *распространялся через Bluetooth или ММ*.

Вирус-Шпион Flexispy

В апреле *2010 года* была обнаружена коварная программа Flexispy, продававшаяся через Интернет за 50 долларов США. Это полнофункциональный шпион, который устанавливает тотальный контроль над смартфоном и начинает

исправно отсылать своему хозяину всю информацию о

Кросс-платформенный вирус Cxover

Это первый мобильный вирус, *способный распространяться в разных операционных системах*. При запуске он определяет ОС, проникает в компьютер и ищет доступные мобильные устройства через ActiveSync. Затем вирус копирует себя на найденное устройство.

Вирус-троян RedBrowser

«Лаборатория Касперского» сообщила о том, что обнаружен вирус, поддерживающий платформу JAVA. Это так называемый троян, получивший название *RedBrowser*.

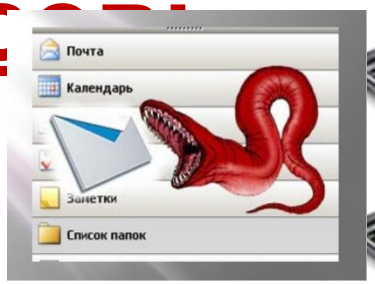
Вирус может быть загружен на телефон как из Интернета с WAP-сайта, так и через Bluetooth-соединение.

Вирус-троян Webster

Вслед за программой RedBrowser в российскую мобильную связь проник ещё один троянец. Называется он *Webster*.

Вирус распространяется в виде файла под названием pomoshnik.jar.

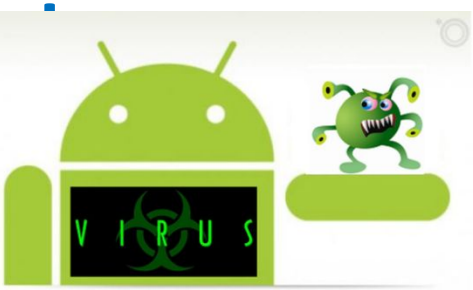
Причины распространения мобильных вирусов



- уязвимости программного обеспечения;
- низкий уровень «мобильной» грамотности;
- отношение владельцев мобильных телефонов к мобильным вирусам, как к проблеме будущего;
- любопытство (а что будет, если я запущу этот файл/игру/программу?);
- несоблюдение элементарных

Пути проникновения вируса в телефон:

- с другого телефона через Bluetooth-соединение;
- посредством MMS-сообщения;
- с ПК (соединение через Bluetooth, USB, WiFi, инфракрасно);
- через w[illegible] сайты.



Симптомы заражения

1. Появление – после копирования и установки каких-либо файлов (как правило, «игр») – всевозможных «глюков» и «багов». *Например:* беспричинно «зависает» телефон, не запускаются какие-либо приложения, невозможно открыть папку *Принятые файлы*.
2. Появление неизвестных подозрительных файлов и иконок.
3. Мобильник самопроизвольно отправляет SMS и MMS, быстро опустошая счет владельца.
4. Блокируются какие-либо

Деструктивные действия мобильных вирусов

Одно из неписаных правил гласит, что вирус, получая управление, может делать в системе всё то, что может делать пользователь!:

- **незаметная для пользователя массовая рассылка *SMS* и *MMS*;**

- **несанкционированные звонки на платные номера;**

- **быстрое опустошение счета абонента (в результате звонков на платные номера и массовой рассылки *SMS* и *MMS*);**

- **уничтожение данных пользователя (телефонная книга, файлы и т.д.);**

- **похищение конфиденциальной информации (пароли, номера счетов и т.д.);**

- **блокировка функций телефона (*SMS*, игры, камера и т. д.) или аппарат в целом;**
- **быстрая разрядка аккумулятора;**

- **рассылка (от имени владельца телефона) зараженных файлов всеми возможными способами (*e-mail*, *WiFi*, *Bluetooth* и т.д.);**
- **при синхронизации телефона с компьютером – пересылка на ПК деструктивного кода;**

Как удалить зараженные файлы

Как правило, непосредственно с мобильника (обычного, не «смарта») удалить зараженные файлы не удается. Для удаления зараженных файлов нужно подключить мобильник к ПК и воспользоваться каким-либо файловым менеджером, например, для телефонов Nokia – *Диспетчером файлов*, входящим в состав Nokia PC Suite. После удаления зараженных файлов перезагрузите мобильник (выключите и снова включите). Если удаление зараженных файлов не помогает, придется «перепрошить» телефон, обратившись в сервисный центр

Как защищаться от мобильных вирусов

1. Если у вас «продвинутый» мобильник, пользуйтесь антивирусами.
2. Соблюдайте осторожность при установке всевозможных приложений (особенно часто мобильные вирусы «молотят» под игры!). Если есть возможность, перед копированием/установкой чего-либо на мобильник, проверьте то, что вы собираетесь копировать/устанавливать, на стационарном ПК антивирусным монитором со свежими базами.
3. Не устанавливайте на мобильник незнакомый «контент» неизвестного происхождения.
4. Не разрешайте запуск незнакомых программ.
5. Не держите Bluetooth постоянно включенным, включайте его только в случае необходимости (а если уж приходится держать Bluetooth постоянно включенным, используйте режим *Скрытый*).
6. Если вам пересылают по Bluetooth какой-то подозрительный файл, вы всегда можете отклонить его прием!
7. Не загружайте файлы из Интернета сразу на мобильник.

Мобильные антивирусы

В то же время решения для защиты от угроз остались и продолжают активно развиваться – антивирусы играют сегодня достаточно заметную роль среди прочих мобильных приложений. Индустрия мобильных антивирусов может предложить целый ряд программных средств по защите ваших сотовых телефонов. Можно вспомнить как отечественные разработки (*Kaspersky Anti-virus Mobile, Dr. Web*), так и зарубежные программы, в частности, от компаний *F-Sec… (F-Secure Mobile Anti-Virus), Syma… (Norton Smartphone Security).*

Выводы:

1. Мобильные вирусы существуют! Это уже не миф, а реальная угроза.

2. До недавнего времени считалось, что мобильные вирусы, если и угрожают, то только продвинуто-навороченным мобильникам, владельцам обычных мобильников бояться нечего. Увы, это уже не соответствует действительности!.. А т.к. доля обычных телефонов как минимум на порядок превосходит долю смартфонов, есть повод задуматься!

3. Поскольку уже созданы кроссплатформенные мобильные вирусы, приверженность какой-то одной ОС не гарантирует защиту от вирусов.

4. Первоначально существовавшая грань между мобильными и компьютерными вирусами стерта. Теперь эти устройства могут взаимно заражать друг друга.

5. Компьютерным вирусам для широкого распространения потребовалось более двадцати лет. Мобильные вирусы прошли этот путь всего лишь за два года (очевидно, что мобильные вирусописатели активно используют опыт создания и распространения компьютерных вирусов).

6. В мире насчитывается около 3 млрд. абонентов сотовой связи. Многие буквально не расстаются со своими мобильниками. На мобильниках хранится конфиденциальная информация. Нетрудно представить масштабы последствий в случае возникновения эпидемий мобильных вирусов.

7. Как относиться к проблеме мобильных вирусов? Не нужно ее преувеличивать, паниковать. Но не стоит и отмахиваться от нее, считая, что проблема искусственно раздувается антивирусными компаниями и жадными до сенсаций СМИ.

Литература

1. https://ru.wikipedia.org/wiki - Википедия
2. http://www.softmixer.com/2011/08/blog-post_8103.html - сетевой журнал
3. http://www.hackzona.ru – территория взлома
4. http://www.mobi.ru – экспертный сайт цифровой техники
5. http://www.vipmks.ru – мобильный корпоративные системы
6. **Создаем вирус и антивирус.** Автор: И.А. Гульев, 304с. – М.: Просвещение, 1999г.
7. **Все о мобильных телефонах: Возможности, выбор, этикет.** Автор: Инджиев А.А. – М.: Феникс, 2006г.

СПАСИБО ЗА ВНИМАНИЕ!