**РЕЧЬ**

Меня зовут Никитчук Кирилл ученик 9 «В» класса средней общеобразовательной школы №10 кадетского корпуса юных спасателей. Руководитель проекта Лысова Тамара Юрьевна, учитель информатики.

Тема моей исследовательской работы «Мобильные вирусы – миф или угроза?»

Представьте себе такую ситуацию: вам срочно нужно позвонить, вы достаёте свой мобильник, собираетесь набрать нужный номер и узнаёте, что у вас на счету нет денег. А ведь всего несколько часов назад баланс составлял целых сто рублей! Что же случилось? Ответ прост: в ваш телефон проник мобильный вирус…

***Вирусы*** – неприятность крайне коварная. Подтвердит любой компьютерщик. Хуже, если дело касается телефона. Тут и контакты, и счёт… и куча других мелочей. Если с ними что-нибудь случится, это парализует всю работу, из средства общения мобильник превратится в глухонемой аппарат.

Данная тема на сегодняшний день является самой актуальной, так проблема вирусов для мобильных телефонов существует уже несколько лет

Работу «мобильные вирусы: миф или реальность?» я выбрал потому, что она меня заинтересовала. Мне было интересно узнать о современном состоянии вирусов для мобильных телефонов.

В своей работе я опираюсь на исследования компьютерных аналитиков и социологические опросы, проводимые антивирусной компанией [McAfee](http://itsecurity.groteck.ru/keywords.php?keyword=5928).

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

**Задачи:**

1. Провести анализ литературы, для изучения проблемы мобильных вирусов.
2. Выяснить, что такое мобильные вирусы?
3. Есть ли реальная опасность подхватить мобильные вирусы на свой мобильный телефон?
4. Что делать, если ваш телефон подхватил мобильный вирус?

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

**Методы:** анкетирование, обработка статистических данных.

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

В своей работе я опираюсь на исследования компьютерных аналитиков и социологические опросы, проводимые антивирусной компанией [McAfee](http://itsecurity.groteck.ru/keywords.php?keyword=5928).

Мной было проведено анкетирование для выявления осведомленности о вирусах для мобильных устройств, среди учащихся 9 классов МБОУ СОШ 10 ККЮС г.Рубцовска, в котором участвовало 22 кадета, в возрасте 15 лет.

**Анкета**

1. **Слышали ли вы о мобильных вирусах?**

Да – 15, нет – 7.

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

Да – 9, нет – 14.

**3. Было ли у Вас заражение телефона вирусом?**

Да – 7, нет – 4, не знаю – 12.

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

Да – 6, нет – 17.

*Анкетирование показало:*

32% - не слышали о мобильных вирусах

63% - не знают каким способом мобильный вирус проникает в телефон

54% - не знают заражен ли у них телефон

77% - не знакомы с антивирусными программами для мобильных телефонов

*Обратимся к истории возникновения мобильных вирусов*

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

2000 год – появление программы Timofonica. Ее нельзя считать полноценным мобильным вирусом, поскольку утилита устанавливалась на компьютер и занималась тем, что рассылала SMS-сообщения.

2000 год – произошел инцидент с несколькими сотнями абонентов японского оператора сотовой связи DoCoMo, мобильные телефоны которых по странной случайности начали звонить в полицию, что привело к перегрузке сети.

2003 году в одном из интервью Евгений Касперский даже позволил себе заявить о маловероятности появления полноценных мобильных вирусов, предназначенных для заражения сотовых телефонов и смартфонов.

Однако в июне 2004 года группой вирусописателей 29А был разработан первый настоящий мобильный вирус – Cabir.

В течение короткого времени для программной платформы Symbian OS были написаны сотни разнообразных вирусов, в числе которых были как черви, так и трояны. Некоторые из них представляли реальную опасность для нормального функционирования мобильных устройств. Видоизменялись и совершенствовались средства распространения вирусов – помимо Bluetooth, заражение происходило за счет MMS-сообщений (первым таким вирусом стал ComWar, появившийся в марте 2005 года).

Спустя месяц после появления вируса Cabir появилось вредоносное приложение для платформы Windows Mobile – Duts, представлявшее угрозу для файловой системы коммуникатора или КПК. Вслед за этим последовали другие Windows Mobile-вирусы, в частности, Brador, ставший первым из мобильных вирусов, открывавшим доступ к зараженному устройству извне. Наконец, чрезвычайно неприятным стало появление в феврале 2006 года RedBrowser – первого мобильного вируса для телефонов с поддержкой Java, что резко увеличивало потенциальную аудиторию зараженных устройств. Вслед за ним появились другие вирусы, такие как, например, Webster.a, представлявший угрозу уже не только для функциональности зараженного телефона, но и для баланса самого владельца – речь идет о потере денег вследствие отправки SMS-сообщений.

Появились и кроссплатформерные вирусы, которые распространялись во время синхронизации с ПК. Если раньше вирусы писались энтузиастами, то постепенно стали появляться настоящие коммерческие разработки. Речь идет, в частности, о краже конфиденциальной информации вроде содержания телефонного справочника или совершенных звонков

**Современное состояние**

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.

Ситуация для мобильных вирусов стала особенно благоприятной с широким распространением смартфонов и коммуникаторов. В отличие от обычного мобильника эти устройства обладают операционными системами, возможностей которых вполне достаточно для того, чтобы стать хорошей средой для распространения вирусов. Bluetooth, через который вирусы способны распространяться особенно быстро.

Особенно активно коварные вирусные программы распространяются в местах массового скопления людей: в метро, в кинотеатрах, в аэропортах. Яркий пример –чемпионат мира по футболу. На огромных стадионах, забитых под завязку, мобильные вирусы распространялись с поразительной скоростью. Многие болельщики стали жертвами этих коварных программ.

Это, пожалуй, лучшая среда для массового заражения мобильников и смартфонов. Во-первых, в таких условиях вирус очень легко распространять. Компьютер, на котором содержится программа-вредитель, просто начинает рассылать её с помощью MMS или Bluetooth всем мобильникам в радиусе от нескольких метров до одного километра. Во-вторых, создаются очень удобные условия для обмана абонентов. Ведь для заражения телефонов недостаточно просто отправить вирус через Bluetooth. Необходимо, чтобы пользователь запустил вредоносную программу на своём телефоне. Реакция увлечённого футбольным матчем человека, которому приходит сообщение о том, что он якобы выиграл билет на следующую игру, вполне предсказуема. Захваченный зрелищем болельщик наверняка даже не почувствует подвоха, нажмёт OK, и зловредная программа попадёт к нему в телефон.

Пока что большинство мобильных вирусов создаются для операционной системы Symbian. Однако эксперты по антивирусным технологиям считают, что помимо данной платформы, соединения Bluetooth и MMS существует еще одна «благоприятная» среда для распространения зловредных программ. Это операционная система Windows Mobile. Она очень уязвима для различных вирусов, так как в ней не существует ограничений для выполняемых приложений. Запущенная программа может запросто получить доступ к любым функциям системы: приёму/передаче файлов, функциям телефонных и мультимедийных служб и т.д. На сегодняшний день известны лишь четыре вида вирусов для этой платформы, но в будущем именно её следует рассматривать как основное поле деятельности мобильных вирусов.

**Червивое разнообразие**

Есть разные виды «инфекций» для мобильных телефонов. Рассмотрим некоторые из них.

### 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. Он быстро может распространяться. Массовый случай заражения этим вирусом произошёл в 2005 году на чемпионате мира по лёгкой атлетике в Хельсинки. На большом стадионе, где проводился чемпионат, Cabir буквально ставил рекорды по скорости распространения. К счастью, сотрудникам финской антивирусной компании F-Secure удалось урегулировать эту ситуацию. На стадионе было отведено специальное место, где телефоны «очищали» от вируса.

### Вирус CommWarrior

В 2005 году появился более опасный вирус назвали CommWarrior. Эта программа довольно долго терроризировала смартфоны абонентов. CommWarrior атаковал Symbian-аппараты на S60 и распространялся через Bluetooth или MMS. Вирус проникал в трубку и сразу начинал рассылать заражённые MMS всем контактам из адресной книги, так как не только выводил аппарат из строя, но и подрывал финансовое положение пользователей несанкционированной рассылкой MMS.

### Вирус-Шпион Flexispy

В апреле 2010 года была обнаружена коварная программа Flexispy, продававшаяся через Интернет за 3000 рублей. Это полнофункциональный шпион, который устанавливает тотальный контроль над смартфоном и начинает исправно отсылать своему хозяину всю информацию о совершенных звонках и отправленных SMS.

### 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. Попав в смартфон, программа пытается проделать обратную процедуру – скопировать себя на персональный компьютер. Вирус может удалять пользовательские файлы на мобильном устройстве.

### 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. Троян маскируется под программу, позволяющую посещать WAP-сайты без настройки, WAP-подключения. Вирус начинает рассылать SMS на платные мобильные сервисы (например, на номера компаний, которые продают игры, мелодии или картинки для мобильников). Стоимость одного такого сообщения может достигать 70 рублей, а отправляются они непрерывно. Таким образом, коварный вирус-троян может за несколько минут попросту разорить абонента. После атаки вируса счёт пользователя обнуляется, а в случае кредитной системы оплаты даже уходит в глубокий минус. «Лаборатория Касперского» отмечает, что вирус ориентирован на абонентов крупнейших российских операторов мобильной связи: МТС, «Билайн» и «МегаФон».

### Вирус-троян Webster

Вирус распространяется в виде файла под названием pomoshnik.jar. Файл этот якобы призван расширить функциональные возможности телефона. Пользователи клюют на такое предложение, запускают «помощника», и вирус проникает в трубку. Как и RedBrowser, Webster поддерживает платформу JAVA. По своим функциям он тоже очень похож на RedBrowser.

### 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 правил безопасности.

### Пути проникновения вируса в телефон:

### с другого телефона через Bluetooth-соединение;

### посредством MMS-сообщения;

### с ПК (соединение через Bluetooth, USB, WiFi, инфракрасное…);

### через web- или wap-сайты.

### Симптомы заражения

### *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*.

### Появление неизвестных подозрительных файлов и иконок.

### Мобильник самопроизвольно отправляет SMS и MMS, быстро опустошая счет владельца.

### Блокируются какие-либо функции телефона.

**Деструктивные (разрушение) 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;

• возможность удаленного управления аппаратом;

### 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.

### *Мной была разработана ПАМЯТКА «Как защищаться от мобильных вирусов»*

### Если у вас «продвинутый» мобильник, пользуйтесь антивирусами.

### 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. Не устанавливайте на мобильник незнакомый «контент» неизвестного происхождения.

### Не разрешайте запуск незнакомых программ.

### Не держите Bluetooth постоянно включенным, включайте его только в случае необходимости (а если уж приходится держать Bluetooth постоянно включенным, используйте режим *Скрытый*).

### Если вам пересылают по Bluetooth какой-то подозрительный файл, вы всегда можете отклонить его прием!

### Не загружайте файлы из Интернета сразу на мобильник. Закачайте их сначала на ПК, проверьте антивирусом, а уж затем устанавливайте в 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-Secure (F-Secure Mobile Anti-Virus), Symantec (Norton Smartphone Security).

**Результаты социологических опросов**.

Как сообщает CyberSecurity, антивирусная компания [McAfee](http://itsecurity.groteck.ru/keywords.php?keyword=5928) провела опрос, согласно которому около 75% пользователей продвинутых сотовых телефонов сообщили, что они всерьез опасаются проникновения в их аппараты мобильных вирусов. Вместе с тем, McAfee замечает, что доля мобильных вирусов в общем их объеме пока ничтожна.

Опрос, проведенный среди пользователей в США, Японии и Великобритании, показал, что лишь 2,1% владельцев телефонов реально сталкивались с мобильными вредоносными кодами. Однако эти пользователи сообщили, что подхватив вирус, они оказались к этому полностью не готовы. Еще 11,6% респондентов сказали, что они знают людей, у которых были проблемы из-за телефонных вирусов. 86,3% сказали, что про [мобильные вирусы](http://itsecurity.groteck.ru/keywords.php?keyword=17806) и прочие угрозы для мобильных телефонов они ничего не слышали.

Вместе с тем, после того, как в McAfee рассказывали пользователям о мобильных вирусах, в среднем 72% говорили об опасности такого явления (в Японии этот показатель заметно выше - 89,1%). Специалисты отмечают, что реакция японского рынка в целом понятна, так как именно там пользователи предпочитают самые последние технические новинки.

**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.