

# Информационная безопасность

# Информационная безопасность

Это совокупность мер по защите  
информационной среды общества и человека.

# Угрозы безопасности данных

```
graph TD; A[Угрозы безопасности данных] --> B[выход аппаратуры из строя]; A --> C[вредоносные программы]; A --> D[ошибки человека];
```

выход  
аппаратуры из  
строя

вредоносные  
программы

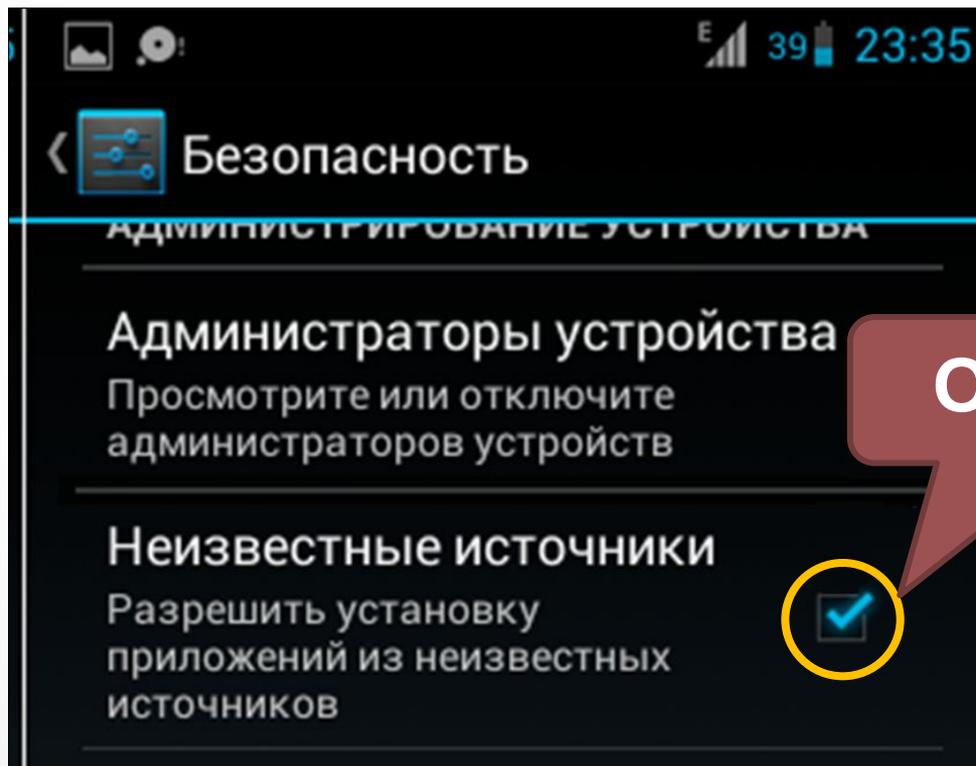
ошибки  
человека

# Безопасность данных

- создание резервных копий файлов;
- установка обновления ос (автообновления);
- использование антивируса;
- отсутствие работы с правами администратора;
- сохранение в тайне своих логина и пароля.

# Безопасность данных

Нельзя устанавливать приложения из неизвестных источников.



**ОПАСНО!**

# Сетевая безопасность

- ❑ проверяйте адреса сайтов;



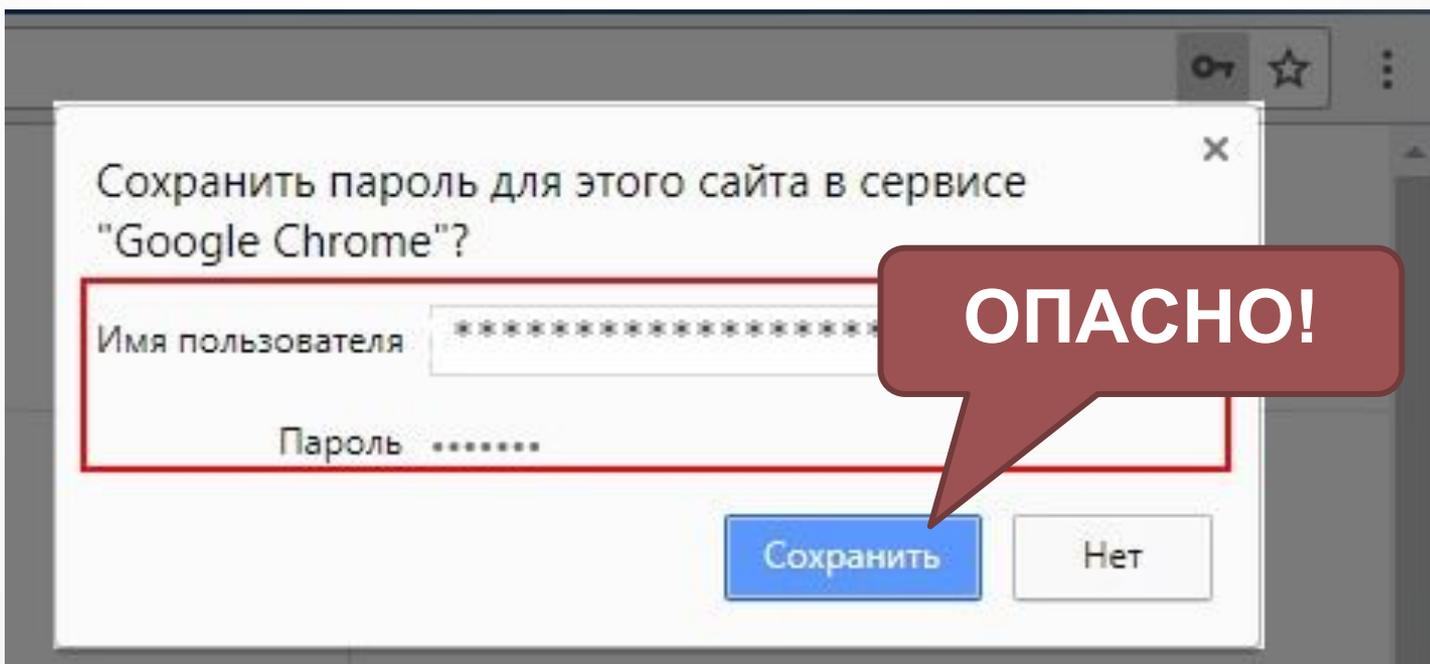
**Другая буква!**

**С шифрованием!**

- ❑ не пересылайте по почте логины и пароли.

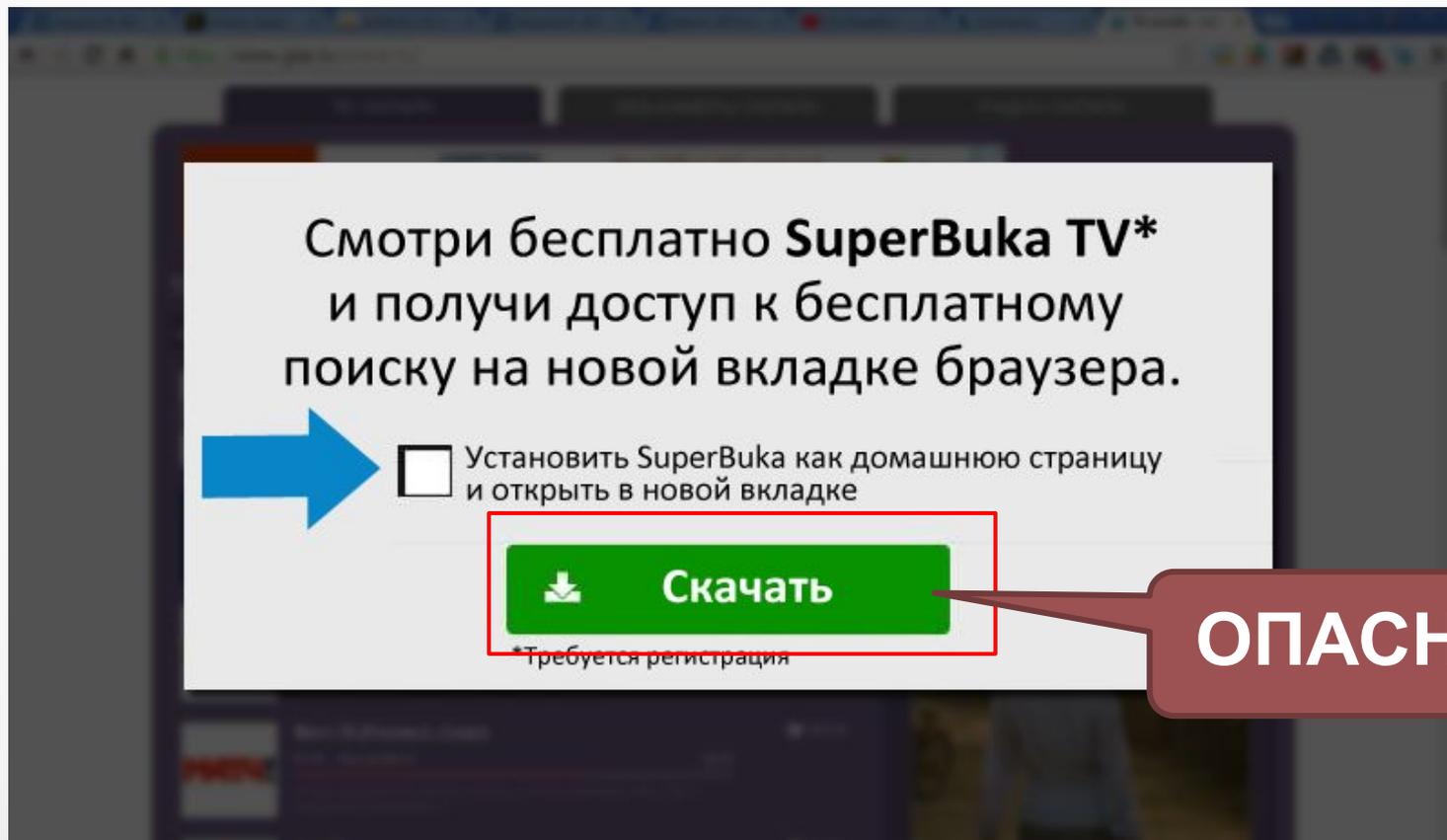
# Сетевая безопасность

Не используйте автосохранение паролей в браузере.



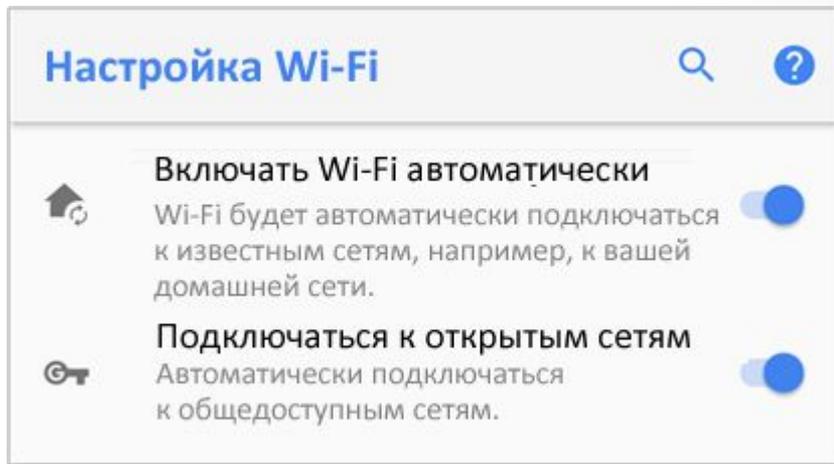
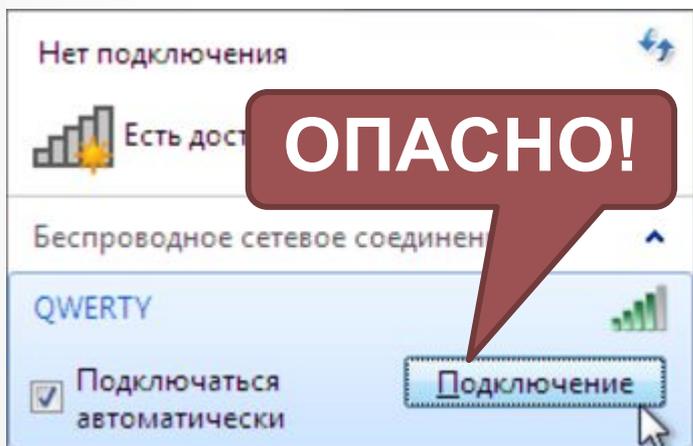
# Сетевая безопасность

Не переходите по ссылкам во всплывающих окнах.



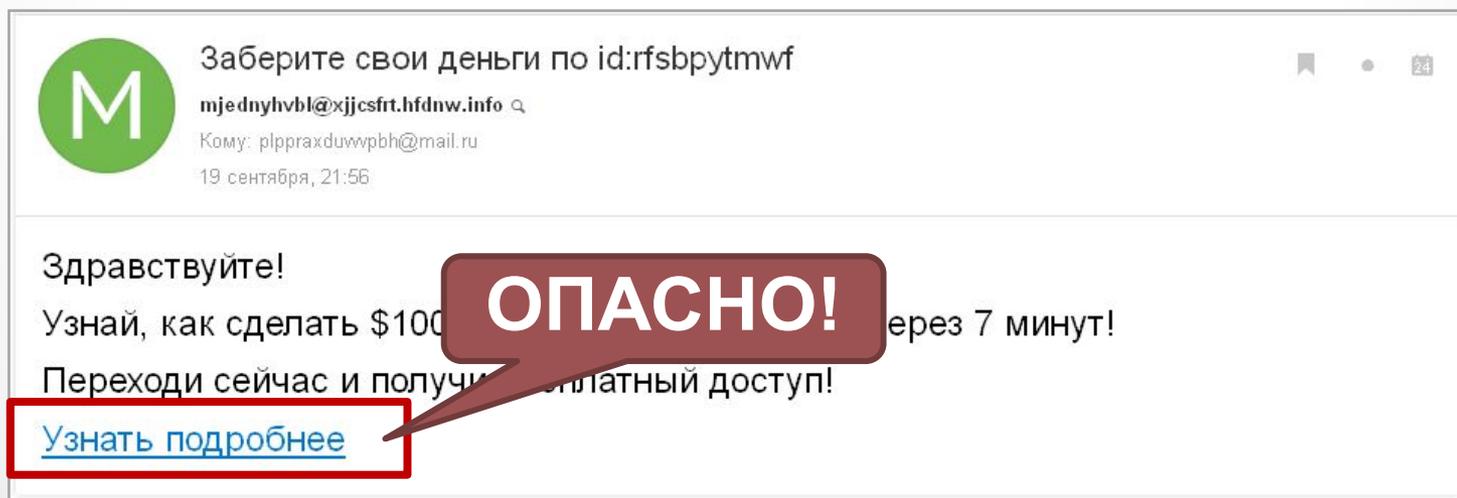
# Сетевая безопасность

Не подключайтесь к беспроводной сети автоматически.



# Электронная почта

- ❑ не используйте основной адрес на форумах, в чатах;
- ❑ не открывайте подозрительные файлы в приложениях к письму;
- ❑ применяйте фильтр спама;
- ❑ не отвечайте на спам.



# Сетевая безопасность

Не вводите номер телефона при скачивании файлов.

Результат запроса\* «драйвера самсунг р518 скачат»:



Рейтинг (7/10)

## Авторизация

Для входа на сайт и снятия ограничений на скачивание файлов, введите номер мобильного телефона.

Введите Ваш номер телефона ниже

Например: +79991223257

 Продолжить

Если у Вас уже есть код, нажмите [здесь](#)

# Мошенничество

- ❑ не переводите деньги за покупки на карты и электронные кошельки;
- ❑ не переходите по ссылкам в сообщении;
- ❑ не отправляйте деньги на неизвестный номер и не звоните по нему.

# Личная безопасность

Нельзя публиковать личные данные в сети.

Василий Пупкин Online  
изменить статус

Контактная информация

|               |                                    |
|---------------|------------------------------------|
| Моб. телефон: | +7(905)123-45-67                   |
| Дом:          | Симферополь, Васильковская ул., 15 |

**ОПАСНО!**

# Личная безопасность

Используйте закрытые профили.



Это закрытый профиль

Добавьте Владимира в друзья, чтобы смотреть его записи,  
фотографии и другие материалы

# Достоверность информации



Не всё, что написано в Интернете, – правда!

## Как проверить:

- сравнить с информацией из книг;
- сравнить информацию с разных сайтов;
- проверить авторитетность сайта;
- посмотреть наличие контактов на сайте;
- посмотреть отзывы на сайт.

# Авторское право

**Цель** – защитить права автора.

В течение жизни и 70 лет после смерти автора,  
потом – всеобщее достояние.

**Не охраняются:**

- официальные документы;
- идеи, методы решения задач;
- алгоритмы;
- языки программирования.

# Компьютерный вирус

Это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.

# Признаки заражения

- замедление работы компьютера;
- перезагрузка или зависание компьютера;
- неправильная работа ОС или прикладных программ;
- изменение длины файлов;
- появление новых файлов;
- уменьшение объема оперативной памяти;
- рассылка сообщений e-mail без ведома автора.

# Вредные действия вирусов

- имитация сбоев ОС и аппаратуры;
- перезагрузка компьютера;
- разрушение файловой системы;
- уничтожение информации;
- шпионаж – передача секретных данных;
- массовые атаки на сайты.

# Способы заражения

- запустить зараженный файл;
- при автозапуске CD(DVD)-диска или флэш-диска;
- открыть зараженный документ с макросами (Word или Excel);
- открыть сообщение e-mail с вирусом;
- открыть Web-страницу с вирусом;
- разрешить установить активное содержимое на Web-странице.

# Классификация компьютерных вирусов по среде обитания

сетевые

файлово-  
загрузочные

файловые

загрузочные

**Классификация  
компьютерных вирусов по  
способу заражения**

```
graph TD; A[Классификация компьютерных вирусов по способу заражения] --> B[резидентные]; A --> C[нерезидентные];
```

резидентные

нерезидентные

# Классификация компьютерных вирусов по степени воздействия

```
graph TD; A[Классификация компьютерных вирусов по степени воздействия] --> B[неопасные]; A --> C[опасные]; A --> D[очень опасные];
```

неопасные

опасные

очень опасные

репликаторы

невидимки

паразитические

**Классификация  
компьютерных  
вирусов по  
особенностям  
алгоритмов**

мутанты

макровирусы

тройные



# Программы-детекторы

Обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение.

# Программы-доктора (фаги)

Не только находят зараженные вирусами файлы, но и «лечат» их (удаляют из файла тело программы вируса, возвращая файлы в исходное состояние).



# Программы-ревизоры

Запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически сравнивают текущее состояние с исходным.



# Программы-фильтры (сторожа)

Представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.



# Программы-вакцины (иммунизаторы)

Это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус.

# Профилактика

- ❑ создание резервных копий;
- ❑ использование антивируса-монитора;
- ❑ при работе в Интернете включение брандмауэра (англ. firewall) – программы запрещающей обмен по некоторым каналам связи, которые используют вирусы;
- ❑ проверка с помощью антивируса-доктора всех новых программ и файлов.

# Вопросы

1. Какие угрозы безопасности данных вы знаете?
2. Что такое «компьютерный вирус»?
3. Какие способы заражения вирусами вы знаете?
4. Какие виды вирусов вы знаете?
5. В чём состоит профилактика заражения вирусами?



**Спасибо за  
внимание!**