**МБУК «ЦБС»**

Центральная городская библиотека

Отдел методической работы

**Защиты от вредоносных программ**



Горячий Ключ

2017

**МБУК «ЦБС»**

Центральная городская библиотека

Отдел методической работы

**Защиты от вредоносных программ**



Горячий Ключ

2017

**МБУК «ЦБС»**

Центральная городская библиотека

Отдел методической работы

**Защиты от вредоносных программ**



Горячий Ключ

2017

**Способы защиты:**

* Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
* Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью дорабтки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
* Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
* Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
* Ограничь физический доступ к компьютеру для посторонних лиц;
* Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проференных источников;
* Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

**Способы защиты:**

* Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
* Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью дорабтки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
* Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
* Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
* Ограничь физический доступ к компьютеру для посторонних лиц;
* Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проференных источников;
* Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

**Способы защиты:**

* Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
* Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью дорабтки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
* Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
* Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
* Ограничь физический доступ к компьютеру для посторонних лиц;
* Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проференных источников;
* Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.