

Подготовка компьютера к безопасному использованию

Автор: Педагог ДД(Ю)Т Московского района г. Санкт-Петербург

Колмогорцев Александр Сергеевич

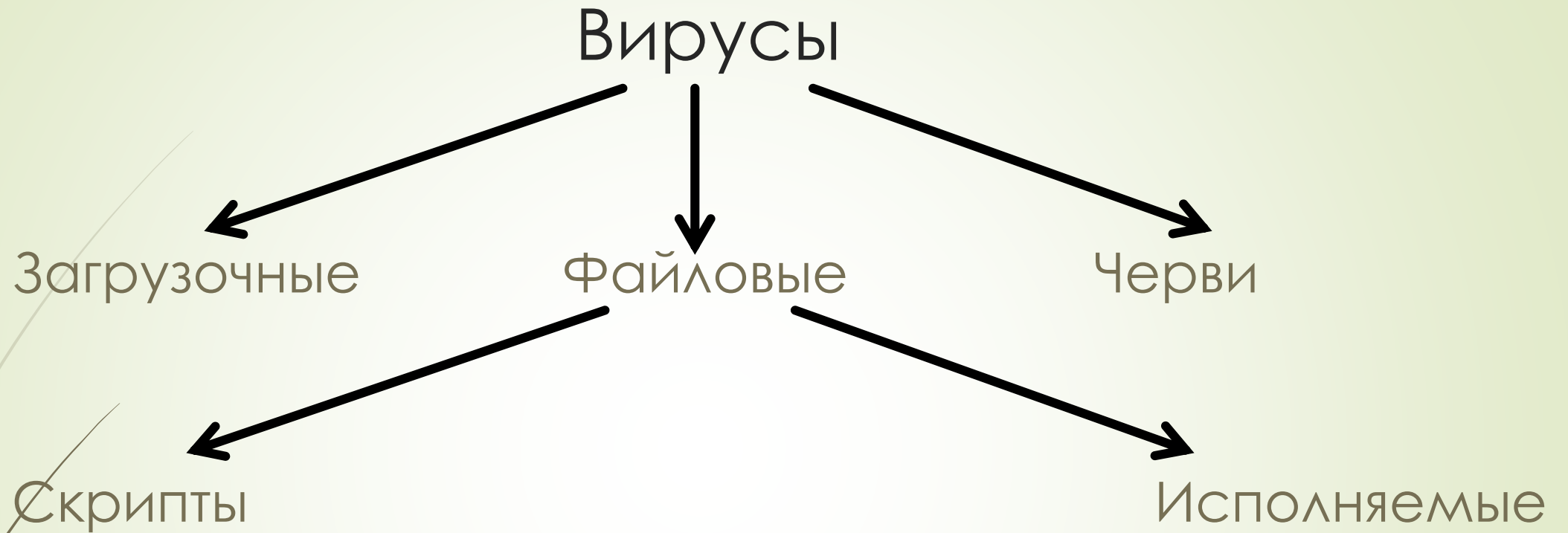
Вирусы

Вредоносные объекты делятся на **вирусы и черви**. Основное отличие в принципе их распространения.

Вирусы попадают на компьютер в основном при запуске какой-то программы. Например, вместе с автозапуском сменных носителей.

Черви же, в свою очередь, попадают на компьютеры пользователей через локальные сети и Интернет.





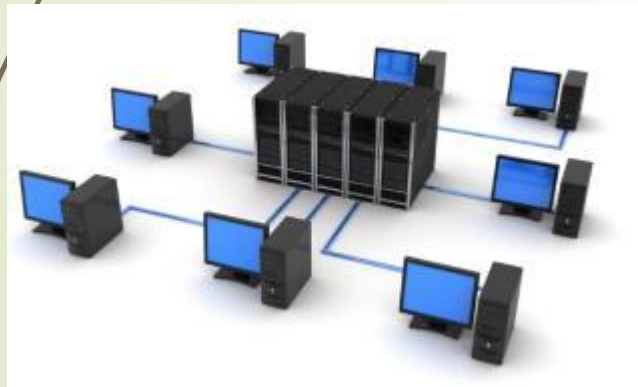
Также существуют комбинации вирусов и червей. В чистом виде вирусов или червей практически не осталось. Чтобы иметь больше шансов на распространение им приходится работать «рука об руку». Именно поэтому часто говорят просто «вирусы» и все.

Пути заражения компьютера

Важная задача пользователя - это знать, что нужно делать, чтобы не заразить компьютер вредоносным объектом. Поэтому важно знать основные пути заражения компьютера.

Пути заражения компьютера:

Локальные сети



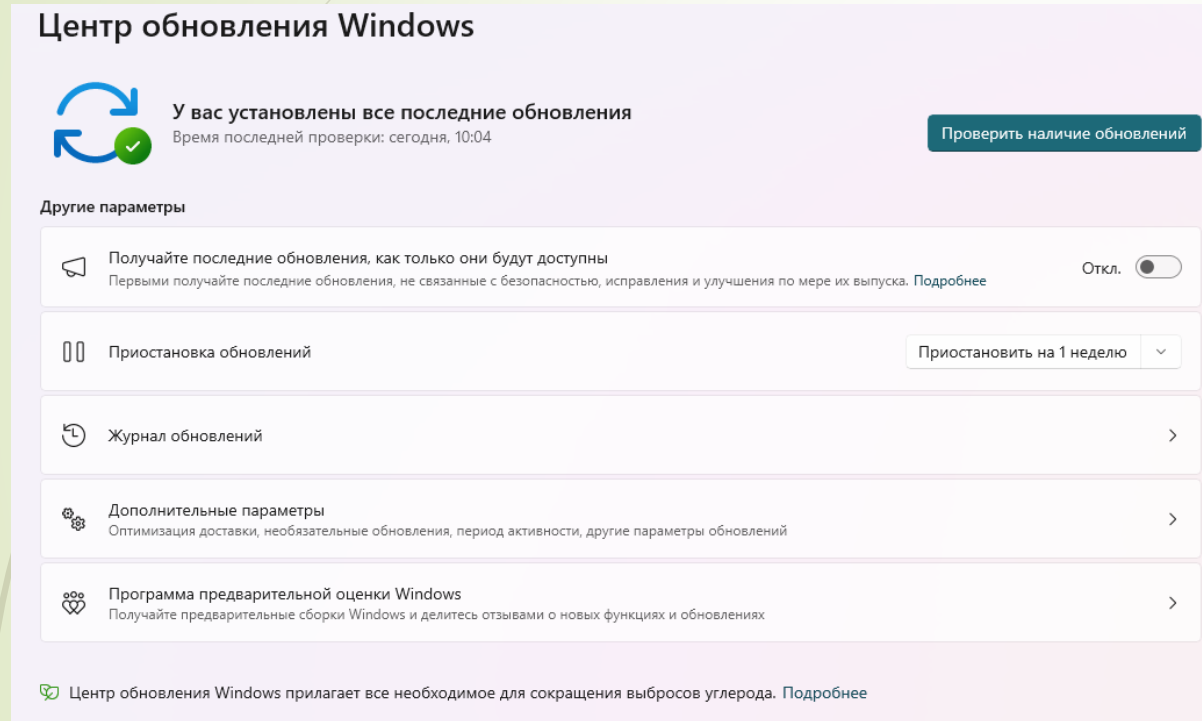
Съёмные носители




Сеть Интернет








1. Обновление Windows




Центр обновления Windows

 У вас установлены все последние обновления
Время последней проверки: сегодня, 10:04 [Проверить наличие обновлений](#)

Другие параметры

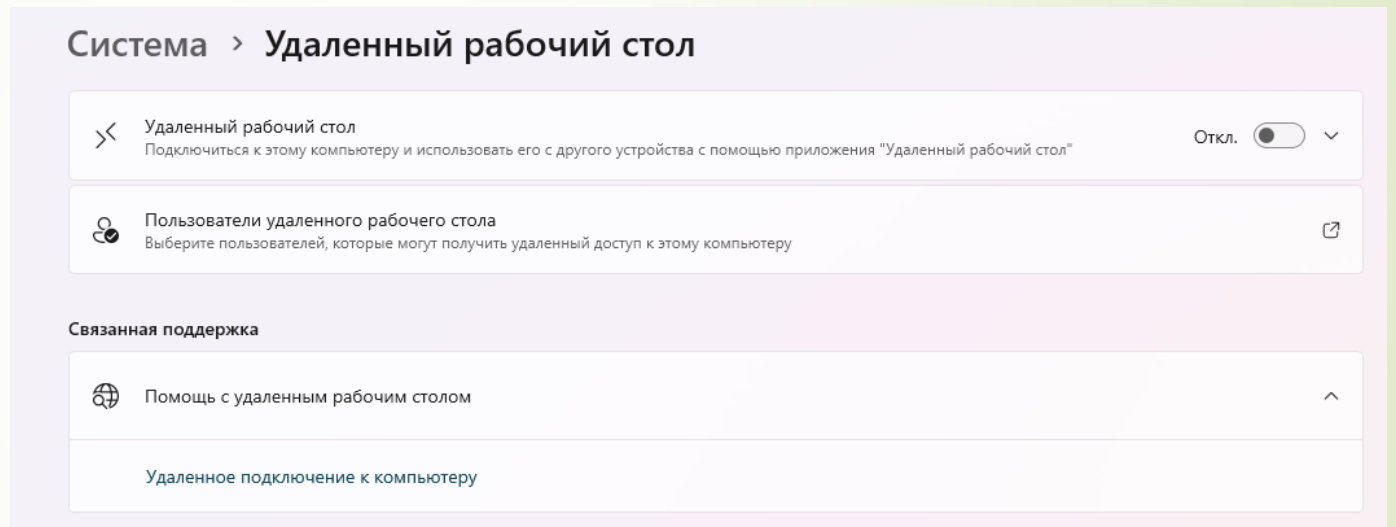
-  **Получайте последние обновления, как только они будут доступны**
Первыми получайте последние обновления, не связанные с безопасностью, исправления и улучшения по мере их выпуска. [Подробнее](#) Откл.
-  **Приостановка обновлений** Приостановить на 1 неделю ▾
-  **Журнал обновлений** >
-  **Дополнительные параметры**
Оптимизация доставки, необязательные обновления, период активности, другие параметры обновлений >
-  **Программа предварительной оценки Windows**
Получайте предварительные сборки Windows и делитесь отзывами о новых функциях и обновлениях >

 Центр обновления Windows прилагает все необходимое для сокращения выбросов углерода. [Подробнее](#)

Проникновение вирусов в операционную систему происходит через ее уязвимости. Так как вирусы находят все новые и новые «дыры» в Windows, то обновления безопасности являются обязательными. Возможно, все обновления устанавливать не обязательно, но установка обновлений безопасности является важным условием на пути в борьбе против вредоносных объектов.

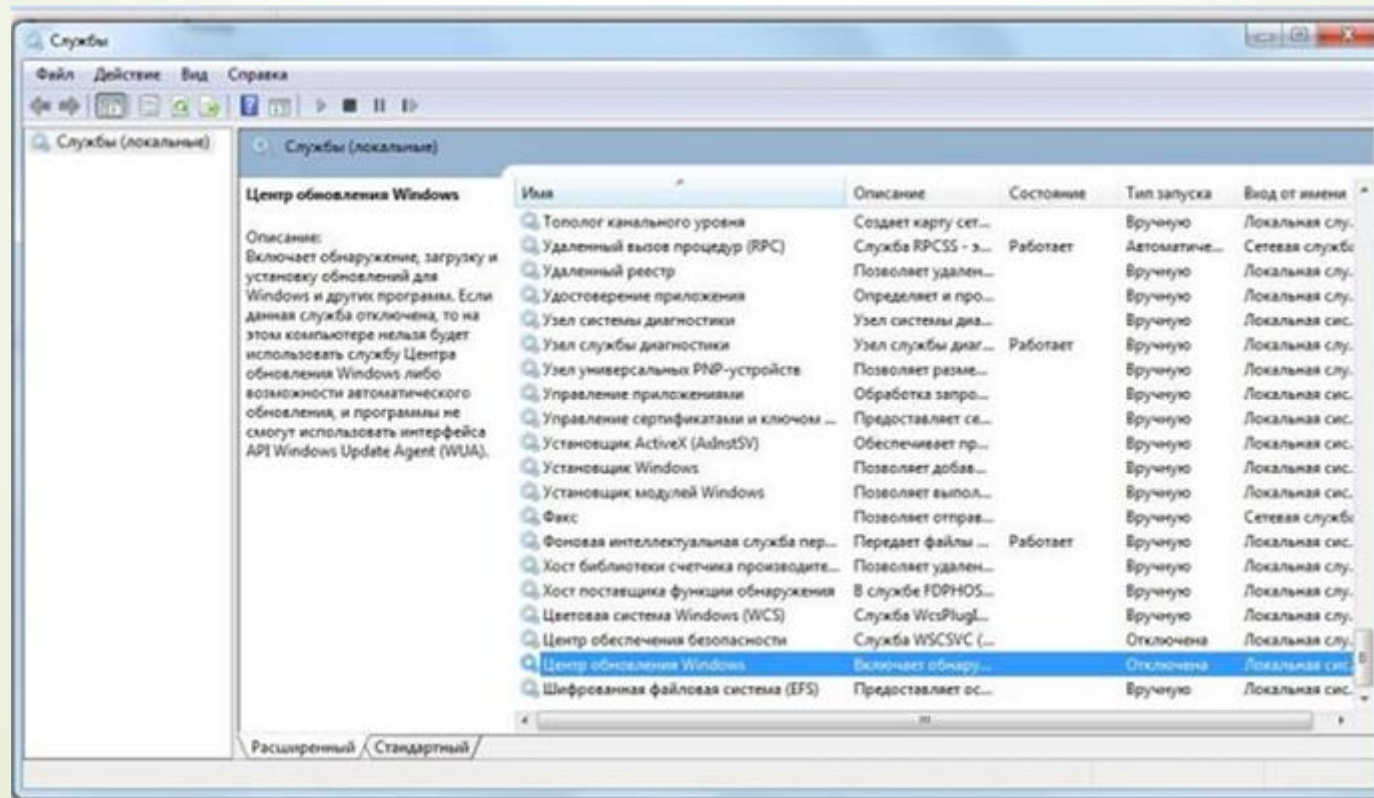
2. Отключение удаленного помощника

Благодаря функции удаленного помощника можно производить подключения удаленно к Вашему компьютеру. Для того чтобы оградить себя от этой уязвимой функции ее желательно отключить и использовать при необходимости сторонние программы.



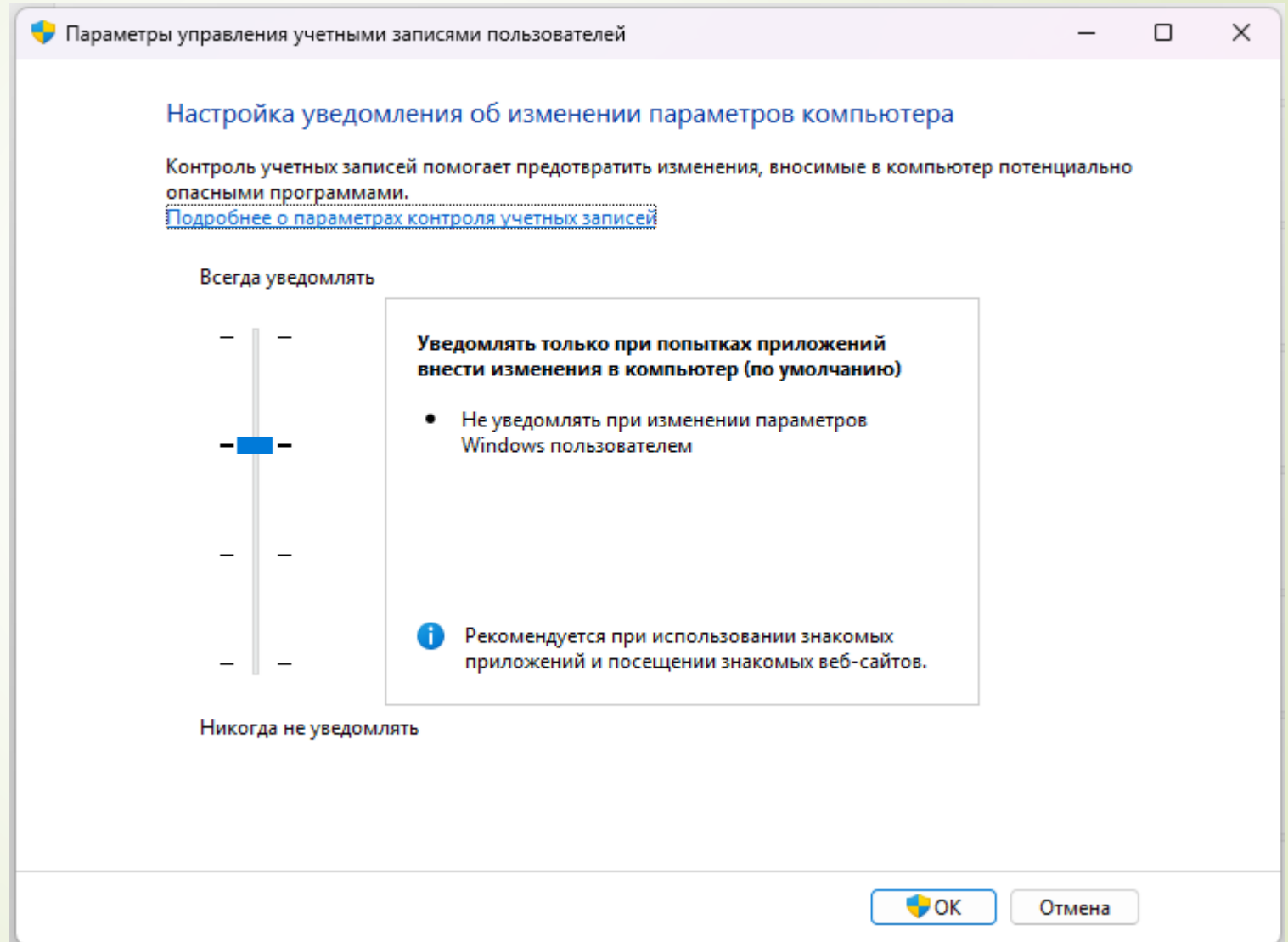
3. Отключение служб Windows

Отключите ненужные уязвимые службы, которые по умолчанию включены в Windows. Например, вот эти службы можно точно отключать: модуль поддержки netbios, настройка сервера удаленных рабочих столов, служба удаленного управления Windows.

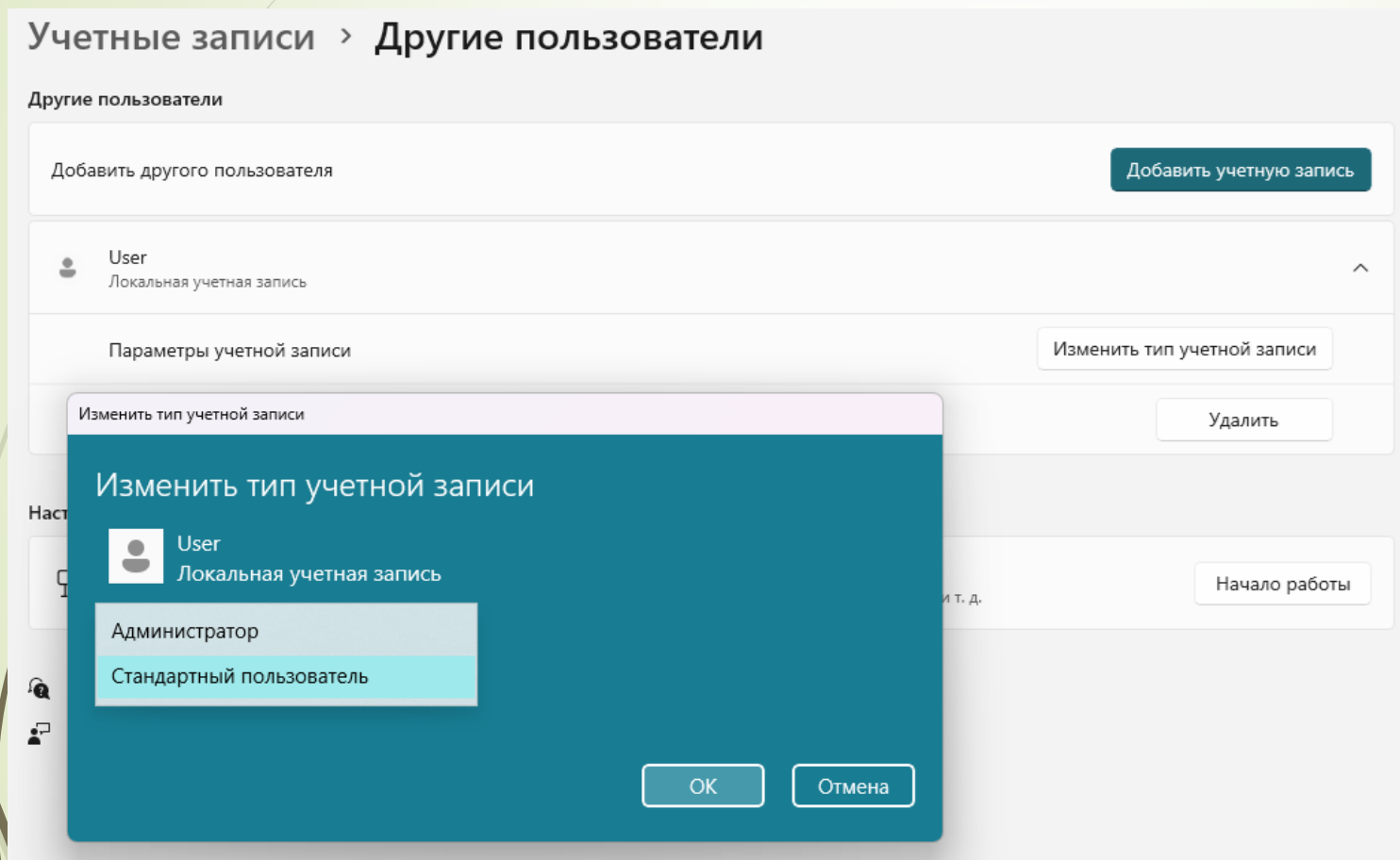


4. Контроль учетных записей

В операционной системе Windows с каждой версией улучшается функция контроля учетных записей. Благодаря этой функции Windows пытается отследить все активности в системе и предупредить пользователя о запуске или установке какой-либо программы. Для надежности и большей безопасности установите контроль выше среднего.



5. Пользователь с ограниченными правами



Это одна из самых важных рекомендаций: создайте второго пользователя в системе с ограниченным (обычным) доступом и в Интернет выход осуществляйте только под этим пользователем.

Если на Ваш компьютер проникнет вирус и перехватит функции пользователя, то он не сможет полноценно осуществлять все функции системе, так как пользователь с ограниченными правами не может изменять системные функции и устанавливать программы.

6. Общественные Wi-Fi сети

При работе в общественных беспроводных сетях (вокзалы, аэропорты, кафе) используйте функцию при подключении к сети «общественная сеть». Находясь подключенным к такой сети, не вводите вручную пароли и логины к своим аккаунтам. Кейлоггеры в таких сетях часто могут считывать всю вводимую Вами информацию.



Неопознанная сеть
Общественная сеть

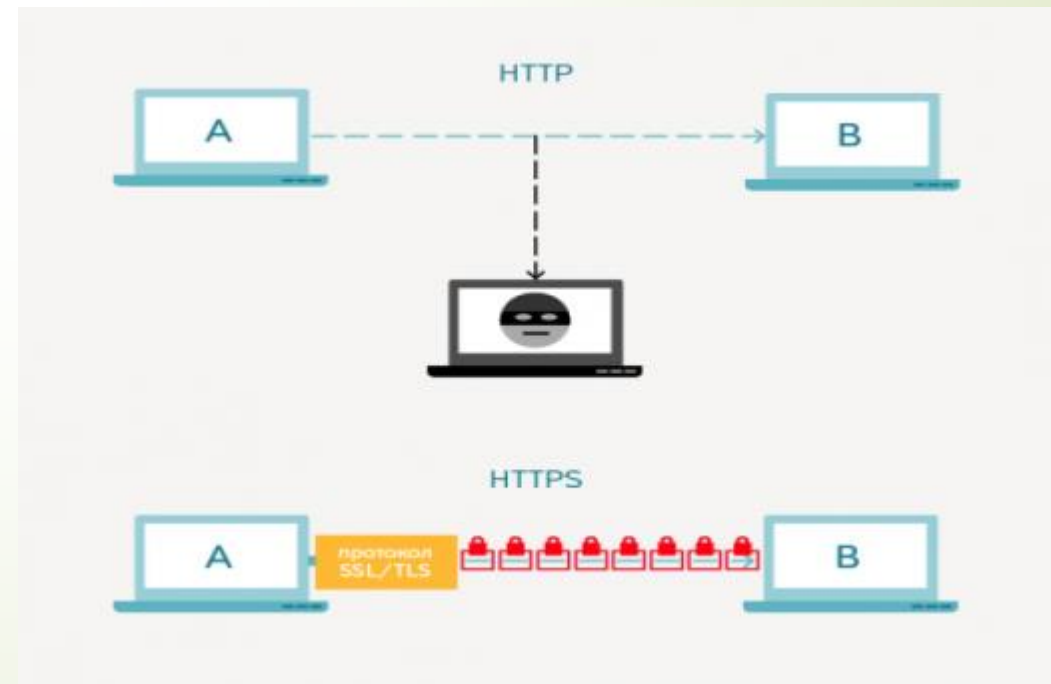
Тип доступа:

Без доступа к
Интернету

Подключения:

Подключение по
локальной сети

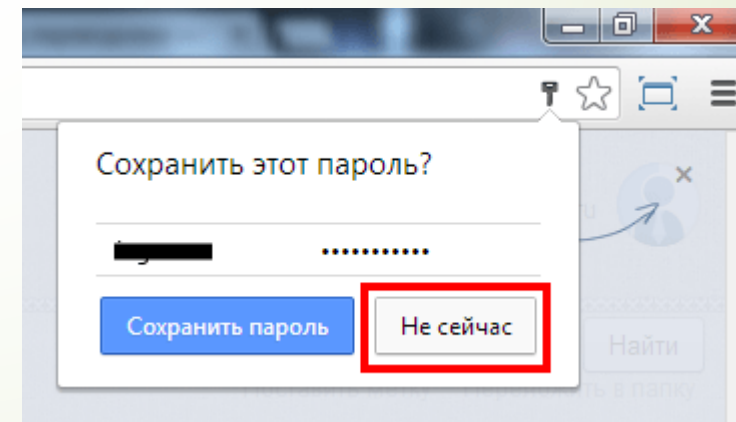
При использовании социальных сетей включайте функцию безопасного соединения по протоколу **https**.



7. Браузеры

Используйте браузер Google Chrome или Mozilla FireFox, именно они являются самыми защищенными. Следите за тем, чтобы браузеры были всегда обновлены.

Очень опасно хранить сохраненные пароли в браузере, Вы даже не представляете, как легко считать все пароли, запустив небольшой троян в систему.



8. Проверка сменных носителей

Производите проверку любым антивирусным средством всех сменных носителей (флешек, дисков) перед тем как их открывать. Также отключите автозапуск всех сменных носителей, так как это основной источник проникновения вирусов с этих носителей.



9. Работа с электронной почтой

Не используйте почтовые программы, пользуйтесь почтой через браузер. Вирусам легче проникнуть в почтовую программу на Вашем компьютере, чем в почту открытую с помощью браузера.



10. Антивирусные программы

Стабильная работа Windows без антивирусных средств это лишь вопрос времени. Большинство пользователей могут длительное время работать без антивируса и не заразиться лишь благодаря счастливой случайности. Важность и необходимость антивируса - это отдельная тема для разговора.



Вывод



Надеюсь Вы примените эти рекомендации на своем компьютере и сами убедитесь, что эти функции гарантированно смогут усилить в несколько раз защиту Вашего компьютера.

