Обеспечение защиты от
вредоносного ПО

- **Методы улучшения защиты от вредоносного ПО и безопасности компьютера**
- Чтобы защитить ваш компьютер от вредоносного ПО:
- Создайте защиту для вашего компьютера
- Не поддавайтесь призывам загрузить вредоносную программу.

- Не поддавайтесь призывам загрузить вредоносную программу.
- **Создайте защиту от вредоносного ПО**
- **Установите антивирусные и антишпионские программы из надежных источников**
- Никогда ничего не загружайте в ответ на предупреждение программы, которую вы не устанавливали или которую не знаете, предлагающей защитить ваш компьютер или удалить вирусы. Велика вероятность заражения вирусами.
- Получайте надежные антивредоносные программы у продавца, которому вы доверяете.
  - Microsoft Security Essentials предлагает бесплатную защиту от вредоносного ПО для вашего ПК в реальном времени.
  - Или Выберите из списка партнеров Microsoft , которые предоставляют антивредоносное программное обеспечение.

- **Регулярно обновляйте программное обеспечение**
- Киберпреступники крайне изобретательны в своих попытках использовать уязвимости в программном обеспечении, и многие разработчики ПО безустанно работают с целью предотвратить эти угрозы. Поэтому вам нужно:
- Регулярно устанавливать обновления для всего вашего программного обеспечения – антивирусных и антишпионских программ, браузеров (таких как Windows Internet Explorer), операционных систем (таких как Windows), программ обработки текстов и прочих программ.
- Включать функции автоматического обновления программного обеспечения, когда таковое доступно, например, вы можете автоматически обновлять все программное обеспечение Microsoft. .
- Удалить программное обеспечение, которое вы не используете. Вы можете удалить его, используя Панель управления Windows.

- **Используйте надежные пароли и храните их в секрете.**
- Надежные пароли должны состоять минимум из 14 символов и содержать сочетание букв, цифр и символов. Узнайте, как их создавать.
- Никому не раскрывайте свои пароли.
- Не используйте одинаковый пароль на всех сайтах. Если его украдут, вся защищенная информация подвергнется риску.
- Создавайте разные надежные пароли для маршрутизатора и ключ беспроводного соединения дома. О том, как это сделать, узнайте в компании, предоставляющей маршрутизатор.

- **Никогда не отключайте брандмауэр.**
- Брандмауэр создает защитный заслон между вашим компьютером и Интернетом. Выключение брандмауэра даже на минуту увеличивает риск заражения ПК вредоносной программой.
- **Осторожно используйте флеш-накопители.**
- Минимизируйте возможность заражения компьютера вредоносным ПО:
- Не вставляйте неизвестные флеш-накопители (или USB-накопители) в свой компьютер.
- Зажимайте клавишу SHIFT, когда вы вставляете накопитель в компьютер. Если вы забыли это сделать, нажмите в верхнем правом углу, чтобы закрыть всплывающие окна флеш-накопителя.
- Не открывайте неизвестные файлы на накопителе.

- **Не соглашайтесь на загрузку, предлагаемую вредоносным ПО.**
- Следуйте данным рекомендациям:
- Будьте очень внимательны, открывая вложенные файлы или нажимая на ссылки в электронной почте, мгновенных сообщениях или в публикациях в социальных сетях (например, Facebook) – даже если вы знаете отправителя. Если отправил друг, позвоните ему и узнайте, он ли это сделал; если нет, удалите или закройте окно службы обмена мгновенными сообщениями.
- Не нажимайте кнопки **«Согласен», «ОК»,** и **«Я принимаю»** в баннерной рекламе, в неожиданных всплывающих окнах или предупреждениях, на сайтах, которые кажутся незаконными, или в предложениях удалить шпионское ПО или вирусы.
  - Нажмите **CTRL + F4** на клавиатуре.
  - Если окно не закрывается, нажмите **Alt + F4** на клавиатуре, чтобы закрыть браузер. Если необходимо, закройте все вкладки и не сохраняйте вкладки для следующего запуска браузера.
- Загружайте программное обеспечение только на сайтах, которым вы доверяете. Остерегайтесь «бесплатных» загрузок музыки, игр, видео и всего прочего. Они известны наличием вредоносного ПО в загрузке.

Коне
ц