Рекомендации по обеспечению безопасности при работе в Сети Интернет

- Не запускайте у себя на компьютере программы из **ненадёжных** источников **и не открывайте приложения к письмам**, даже если письмо пришло от Вашего хорошего знакомого: в них могут быть спрятаны вирусы или троянские кони. Присланные вам файлы или ссылки могут быть заражены – не открывайте их! **Сначала сохраните приложение или файл на компьютер и проверьте его антивирусной программой.** Помните, что злоумышленники могут прибегнуть к разнообразным приёмам, чтобы обманом получить у Вас информацию об идентификационных параметрах. Тщательно проверяйте имена сайтов, на которые переходите по ссылкам.

- Не надо верить всем сообщениям о новых страшных вирусах, появившихся в Интернет, особенно если в сообщении сказано, что надо распространить эту информацию всем Вашим знакомым. Это сообщение может оказаться носителем вируса или просто компьютерной шуткой.

- Если Вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего это спам - назойливые рекламные письма - и письмо попало в Ваш ящик не по ошибке, а специально. Чтобы не получать письма от этого адресата впредь, нужно добавить для него соответствующий фильтр с последующим автоматическим удалением писем от него или добавить адресата в «чёрный» список.

- Обязательно установите на ВСЕ компьютеры антивирусную программу для защиты от троянских коней и вирусов в режиме резидентного монитора (тогда она будет проверять все запускаемые программы и открываемые документы автоматически). Помните, что **бесплатные** версии антивирусов по условия их лицензий можно устанавливать ТОЛЬКО на ДОМАШНИИ компьютеры для личного пользования. В образовательном учреждении рекомендуем использовать Kaspersky Endpoint Security 10 for Windows (http://www.kaspersky.ru/product-updates). Обновляйте антивирусные базы данных не реже, чем каждые 3-5 дней. Если антивирусная база не обновлялась более 3 месяцев, эффективность антивируса сильно снижается.

- Ограничьте доступ к Вашему компьютеру с помощью установки безопасности (запрос пароля при входе в систему Windows).

- Делайте резервные копии системных файлов и важных данных и храните их в безопасном месте (не на жёстком диске Вашего компьютера). В случае сбоя жёсткого диска или вирусной атаки это позволит Вам быстро восстановить систему (данные) и продолжить работу.

- Помните, что программы, которыми Вы пользуетесь при работе в Интернет, могут содержать ошибки безопасности ("дыры"). Эти ошибки могут позволить злоумышленнику заблокировать Ваш компьютер или получить несанкционированный доступ к нему через Интернет. Производители операционных систем и прикладных программ регулярно публикуют информацию об обнаруженных "дырах" (например, www.microsoft.com) и исправленные версии программ. Проверьте, что Вы установили ВСЕ исправления для используемых Вами программ, и если нет - сделайте это как можно скорее. Следите за публикациями о новых обнаруженных ошибках в программах и оперативно устанавливайте исправления для них.

- Не думайте, что вирусы и троянские кони могут находиться только в программах, загруженных из Интернета - как показывает печальный опыт использования пиратских CD и пиратских программ, скачанных из сети Интернет, на них все чаще появляются программы, также заражённые вирусами или троянскими конями. Если уж Вы купили CD или скачали программу из сети Интернет, проверьте его хорошей антивирусной программой с последней антивирусной базой данных.

    - Более подробную информацию об угрозах подстерегающих пользователей сети Интернет можно познакомиться на сайтах «Dr.Web» (http://www.freedrweb.com/aid_admin/) или «Лаборатории Касперского» http://www.kaspersky.ru/internet-security-center. Используйте бесплатные специализированные программы для лечения и проверки компьютера на вирусы, например:

        - Лечение зашифрованных файлов (Для расшифровки данных, заблокированных программами-шифровальщиками, используйте утилиты XoristDecryptor и RectorDecryptor)

        - Разблокировка компьютера (Для удаления баннера блокера-вымогателя с рабочего стола, используйте утилиту Kaspersky WindowsUnlocker.)

        - Удаление руткитов (Для лечения компьютера от программ, перехватывающих системные функции, используйте утилиту TDSSKiller)

- Kaspersky Rescue Disk (Бесплатный продукт поможет вам вылечить и восстановить систему при критическом заражении).
- Dr.Web LiveDisk (бесплатная утилита для восстановления работоспособности компьютера после вирусной атаки, в результате которой доступ к рабочему столу оказался заблокированным, а операционная система перестала загружаться или работает не стабильно. Поддерживаются ОС Windows 2000 — Windows 8, а также Unix и Linux)
- Утилиты от троянских программ Dr.Web:
  - Сервис разблокировки Windows от Trojan.Winlock
  - Утилита от Trojan. Plastix
  - Утилита сбора информации о системе.