Памятка по информационной безопасности

при работе в социальных сетях (в сети Интернет)

- **Не публикуйте личные и конфиденциальные сведения**
  Не пересылайте пароли, логины, паспортные данные, ПИН-коды и прочую подобную информацию в соцсетях, мессенджерах, чатах или по электронной почте.
- **На ПК должны быть установлены антивирусные программы**
  - Необходимо контролировать наличие антивирусной программы, актуальность обновлений.
  - При подключении к рабочему компьютеру внешних носителей информации проверяйте их содержимое с помощью средств антивирусной защиты
- **Не устанавливайте сомнительные приложения**
  Используйте безопасные источники приложений и официальные сайты компаний, разработавших приложения.
  Установка приложений из других источников, в том числе различных ломаных и пиратских версий, может закончиться тем, что вам придется тщательно чистить компьютер или телефон от вирусов.
- **Проверяйте безопасность соединений**
  Всегда обращайте внимание на то, что написано в адресной строке. Если вы видите, что адрес сайта начинается с HTTPS – все в порядке, это безопасное соединение и здесь можно вводить конфиденциальную информацию. Если же адрес начинается с HTTP – это значит, что соединение не защищено. Также слева от HTTPS должен быть значок в виде замка. Для большей уверенности в безопасности соединения можно кликнуть на него и просмотреть информацию во всплывающем окне.
- **Используйте сложные логины и пароли**
  - длина пароля должна быть не менее 8 символов;
  - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
  - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.);
  - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.
  - Личный пароль пользователь не должен никому сообщать.
  - Периодичность смены пароля не должна превышать 90 календарных дней.
  - Пароли должны быть уникальными: не используйте один и тот же пароль для всех рабочих ресурсов. Тем более — не используйте его же и в личных целях. Достаточно будет утечки из одного из сервисов, чтобы скомпрометировать их все.
  - Пароли должны быть секретными: не записывайте пароль на бумаге и не храните около рабочего места; не вписывайте их в файлы и не делитесь ими с коллегами.
- **По возможности использовать двухфакторную аутентификацию**
- **Не применяйте имена пользователей и пароли служебных компьютеров на личных устройствах;**
- **Не публикуйте служебные электронные адреса (в т.ч. из домена gov35.ru) на досках объявлений, в конференциях и гостевых книгах;**
- **Не нажимайте на баннеры, которые заставляют вас загружать дополнительное программное обеспечение.**
  Если вы нажали на «крестик», а вместо этого перешли на новый сайт – немедленно закройте окно браузера.
- **Разлогинивайтесь на чужих устройствах**
  Воспользовались чужим компьютером? После этого недостаточно просто закрыть страницу, на которую вы заходили. Не забывайте предварительно выходить из всех аккаунтов, соцсетей и мессенджеров на устройстве. В противном случае человек, который сядет за этот компьютер после вас, получит возможность войти в вашу учетную запись и сделать с ней все, что ему заблагорассудится.
- **Выключайте Bluetooth-соединение и другие методы передачи данных на смартфонах, когда ими не пользуетесь.**