Памятка по соблюдению ЦИФРОВОЙ ГИГИЕНЫ

1. Электронная почта

1. Для обмена информацией использовать только служебную электронную почту.
2. Не допускается использование сторонних электронных сервисов и ресурсов, таких как google.com, yandex.ru, mail.ru, yahoo.com, live.com, для обмена и хранения служебной информации.
3. При получении письма по электронной почте необходимо проверить его на наличие следующих признаков, характерных для спам-писем:
   - письмо получено от неизвестного адресанта;
   - в строке получателей много неизвестных адресатов либо адресаты подобраны без смысла (например, все адресаты письма имеют имя «Елена»);
   - письмо написано на иностранном языке;
   - тема и содержимое письма не совпадают;
   - письмо содержит рекламную информацию;
   - к письму приложен архив или файлы с двойным расширением (например, «резюме.docx.scr», «акты.zip.txt»);
   - иконка приложенного файла не соответствует его расширению;
   - в письме предложено перейти по ссылке для скачивания файлов либо перехода на внешний Интернет-ресурс.
4. Во избежание заражения компьютера Вы не должны открывать вложения и переходить по ссылкам в письмах, имеющих признаки спам-сообщений.

2. Парольная политика

1. Пароль не должен быть легко вычисляемым (например, 12345678, password, Ваше имя, дата рождения, другая личная информация).
2. Рекомендуемая длина паролей – не менее 8 символов, также необходимо использовать различные символы (строчные и прописные буквы, цифры, специальные символы).
3. При смене на новый, пароль должен отличаться от предыдущего не менее чем на 3-4 символа.
4. Пароль должен меняться не реже чем один раз в три месяца.
5. Запрещается оставлять свой пароль в общедоступных местах.
6. Запрещается передавать свой пароль третьим лицам.

3. Используемое программное обеспечение

1. В рабочей деятельности необходимо использовать только лицензированное программное обеспечение.
2. На автоматизированном рабочем месте (далее – АРМ) должен быть установлен минимальный набор программного обеспечения необходимого для исполнения служебных обязанностей.
3. Не допускать использование программного обеспечения, не предназначенного для исполнения служебных обязанностей.
4. Запрещено самостоятельно устанавливать и/или настраивать программное обеспечение на АРМ.
5. При необходимости обновления системного и прикладного программного обеспечения – обращаться к системному администратору для выполнения обновлений.

4. Работа в сети «Интернет»

1. Перед началом работы в сети «Интернет» необходимо убедиться в наличии и корректном функционировании средства антивирусной защиты информации, установленного на АРМ (отсутствие сообщений об ошибке, актуальная антивирусная база).
2. При работе в сети «Интернет» необходимо обращать внимание:
    - на всплывающие окна с различным содержанием (не вводить свои личные данные (логины, пароли, данные пластиковых карт, контактные телефоны и т.д.), кликать на них для перехода на другие страницы);
    - на адрес сайта, указанный в адресной строке (соответствие адреса сайта с запрашиваемым, например, отображение вместо привычного адреса в адресной строке – sberbak-online.ru);
    - на загружаемые файлы (непреднамеренная загрузка, загрузка без Вашего согласия и т.д.).
3. В случае, если при работе в сети «Интернет» средство антивирусной защиты выдало ошибку, либо уведомляет о каком-то подозрительном действии, необходимо незамедлительно прекратить работу в сети «Интернет» и сообщить об этом системному администратору, либо администратору безопасности.

5. Средства защиты информации

1. Пользователь обязан перед началом работы проверить наличие и работоспособность всех средств защиты информации, установленной на АРМ.
2. В случае обнаружения отсутствия какого-либо средства защиты информации, либо его неработоспособность (при наведении на иконку выдается сообщение о какой-либо ошибке, либо невозможности запустить данную службу, программу).
3. В любом из вышеуказанных случаев пользователь обязан:
    - прекратить работу с АРМ;

- проинформировать об отсутствии или неработоспособности средства защиты информации системного администратора, либо администратора безопасности;
- дождаться устранения проблемы связанной с средством защиты информации и после устранения приступить к работе с АРМ.

6. Инциденты

1. Незамедлительно обратиться к системному администратору, либо администратору безопасности при нештатной работе АРМ выражающейся:
   - в периодическом зависании;
   - в спонтанном открытии диалоговых окон;
   - в самопроизвольном запуске различных приложений.
2. При обнаружении исчезновения файлов и/или папок на сетевом ресурсе (сетевой диск) необходимо незамедлительно сообщить о данном факте системному администратору, либо администратору безопасности и прекратить работу с сетевым ресурсом.
3. При обнаружении исчезновения файлов и/или папок на АРМ необходимо незамедлительно сообщить о данном факте системному администратору, либо администратору безопасности, прекратить работу с АРМ, отключить его от электропитания и от локально-вычислительной сети.

7. Корпоративная связь

1. Не допускается использование средств корпоративной связи в личных целях.
2. Не допускается использование корпоративный номер для регистраций на сторонних сервисах и ресурсах.
3. При получении смс сообщений обращать внимание на отправителя и содержание самого сообщения, не переходить по ссылкам и не сообщать третьим лицам полученную парольную информацию.
4. При входящих звонках с незнакомых номеров, а также номеров, принадлежащих операторам связи, находящихся за пределами территории РФ, соблюдать предельную осторожность и не разглашать какую-либо служебную и личную информацию.