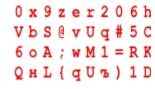
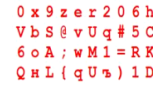
# ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.  **Не допускайте просмотра** информации посторонними лицами с **монитора компьютера**. Покидая рабочее место, выключайте или блокируйте компьютер.
2.  **Не допускайте установку и запуск программного обеспечения** без согласования с системным администратором.
3.  **Работайте** только **под своей учетной записью**!
4.   **В случае попытки** посторонних лиц **выведать** у Вас любую конфиденциальную информацию, **не разглашайте её и сообщите об этом** своему непосредственному руководителю.
5.   **Придумывайте длинные и сложные пароли**! Пароль не должен содержать легкоподбираемые слова (логин, имя, фамилия, даты и т.д.).
6.  **Храните в тайне** атрибуты подключения (логины, пароли, наименования серверов, IP-адреса и т.п.).
7.  **Не оставляйте без контроля** документы, съемные носители, ноутбуки в общедоступных местах, даже на короткий срок.
8.  **Соблюдайте политику чистого стола!** Если покидаете рабочее место - закройте помещение, уберите в запираемый шкаф документы, съемные носители, ноутбуки.
9.  **Не работайте на компьютере без антивируса!** Проверяйте его наличие при запуске системы.
10.  Избегайте использования съемных носителей (**флешки, диски, mp3-плееры, телефоны и т.п.**), особенно чужих. **Обязательно проверьте** их **антивирусом** перед началом работы.
11.   **Воздержитесь от использования Интернета** без производственной необходимости. Сайты могут содержать опасные вирусы!
12.   При получении электронного сообщения из незнакомого источника **не следует открывать вложенные в сообщение файлы.** Скорее всего, в них содержится вирус. Удалите письмо.
13.  Нежелательно использование в рабочих целях сервисов иностранных Интернет-компаний, в том числе для пересылки конфиденциальной информации.
14.  Любую **конфиденциальную информацию,** в том числе персональные данные**, пересылайте только по защищенным каналам связи**


# ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.  **Не допускайте просмотра** информации посторонними лицами с **монитора компьютера**. Покидая рабочее место, выключайте или блокируйте компьютер.
2.  **Не допускайте установку и запуск программного обеспечения** без согласования с системным администратором.
3.  **Работайте** только **под своей учетной записью**!
4.   **В случае попытки** посторонних лиц **выведать** у Вас любую конфиденциальную информацию, **не разглашайте её и сообщите об этом** своему непосредственному руководителю.
5.   **Придумывайте длинные и сложные пароли**! Пароль не должен содержать легкоподбираемые слова (логин, имя, фамилия, даты и т.д.).
6.  **Храните в тайне** атрибуты подключения (логины, пароли, наименования серверов, IP-адреса и т.п.).
7.  **Не оставляйте без контроля** документы, съемные носители, ноутбуки в общедоступных местах, даже на короткий срок.
8.  **Соблюдайте политику чистого стола!** Если покидаете рабочее место - закройте помещение, уберите в запираемый шкаф документы, съемные носители, ноутбуки.
9.  **Не работайте на компьютере без антивируса!** Проверяйте его наличие при запуске системы.
10.  Избегайте использования съемных носителей (**флешки, диски, mp3-плееры, телефоны и т.п.**), особенно чужих. **Обязательно проверьте** их **антивирусом** перед началом работы.
11.   **Воздержитесь от использования Интернета** без производственной необходимости. Сайты могут содержать опасные вирусы!
12.   При получении электронного сообщения из незнакомого источника **не следует открывать вложенные в сообщение файлы.** Скорее всего, в них содержится вирус. Удалите письмо.
13.  Нежелательно использование в рабочих целях сервисов иностранных Интернет-компаний, в том числе для пересылки конфиденциальной информации.
14.  Любую **конфиденциальную информацию,** в том числе персональные данные**, пересылайте только по защищенным каналам связи**