



данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

- Не произносите вслух, не записывайте и не храните в любом доступном посторонним лицам месте пароли.

## 2.2. В целях защиты персональных компьютеров:

- используйте только лицензионное системное и прикладное программное обеспечение;
- установите на компьютер только одну операционная система;
- не устанавливайте и не используйте на компьютере программы для удаленного управления, например TeamViewe;
- установите и регулярно обновляйте антивирусные программы (например, Kaspersky, Dr.Web, Symantec, Avira, ESET, NOD 32, McAfee).
- своевременно проводите обновление системного и прикладного программного обеспечения.
- для доступа к информационным системам не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее)
- при передаче информации с использованием чужих компьютеров, после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились;
- не передавайте персональных данных и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами;
- не переходите по ссылкам в таких письмах, не открывайте вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение);
- в случае обнаружения подозрительных действий, совершенных в компьютере, незамедлительно смените логин и пароль;
- при обнаружении совершения незаконных финансовых операций – незамедлительно подайте заявление о данном факте в правоохранительные органы и сохраните доказательства данного факта в устройстве.
- при работе с иными носителями информации перед началом работы осуществляйте их проверку на предмет отсутствия компьютерных вирусов.

## 2.3. В целях защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники:

- обновляйте антивирусные программы на постоянной основе;
- осуществляйте регулярный контроль работоспособности антивирусных программ;
- создайте условия, при которых невозможно несанкционированное отключения средств антивирусной защиты;
- антивирусная защита должна обеспечивать сохранение безопасного состояния информации при любых сбоях;
- вынесите ярлык для запуска антивирусной программы на рабочий стол персонального компьютера и используйте его регулярно.



**ООО МЖК ТАНОС**

Проинуровано, пронумеровано и скреплено

печатью

2 листа

Генеральный директор

*Шушкина К. А.*  
Шушкина К. А.