

**Рекомендации по защите информации**

**Уважаемый предприниматель!**

Предлагаем Вам ознакомиться с мерами, направленными на предотвращение несанкционированного доступа к защищаемой информации со стороны третьих лиц, не обладающих правом осуществления финансовых операций, которые позволят Вам защитить информацию и обезопасить проводимые Вами финансовые операции.

Под защищаемой информацией понимается:

* информация, содержащаяся в документах, составляемых Вами при осуществлении финансовой операции в электронном виде,
* информация об осуществлении Вами финансовых операций,
* ключевая информация средств криптографической защиты информации (СКЗИ), используемой Вами при осуществлении финансовых операций,
* Ваши персональные данные.

В случае утраты (потери или хищения) документов, удостоверяющих Вашу личность или других документов, содержащих личную информацию **возможен риск** использования Ваших персональных данных мошенниками в собственных корыстных целях, в том числе для совершения финансовых операций от Вашего имени.

**Рекомендуем** надежно хранить личные документы и обдуманно распространять личную информацию**.**

При утрате (потери или хищении) электронных устройств (персональных компьютеров, мобильных телефонов и пр.) (далее - электронные устройства), используемых Вами в целях осуществления финансовой операции, **возможен риск получения несанкционированного доступа к защищаемой информации.**

В качестве мер по предотвращению несанкционированного доступа к защищаемой информации с помощью электронных устройств, используемых Вами в целях осуществления финансовой операции, **рекомендуем Вам следующее**:

* надежно хранить электронные устройства в целях избежания их утраты (потери или хищения);
* не позволять пользоваться электронными устройствами посторонним лицам;
* устанавливать на электронные устройства надежные пароли доступа и блокировки;
* не разглашать коды, пин-коды и т.д. посторонним лицам;
* использовать на электронных устройствах надежные антивирусные программы и регулярно проводить обновление антивирусных баз, а также не менее одного раза в неделю проводить полную проверку электронных устройств с применением обновленных баз. Данная мера позволит своевременно обнаружить воздействие вредоносных кодов, уничтожить вредоносный код и защитить устройство от заражения;
* не посещать подозрительных сайтов, не проходить по ссылкам во вложении к электронным письмам от незнакомых адресатов, т.к. данные действия могут увеличить риск заражения Вашего устройства вредоносным кодом.
* при утере электронных устройств или выявлении случая несанкционированного доступа к электронным устройствам как можно быстрее сообщить об этих фактах в финансовые учреждения, с которыми Вы сотрудничаете.

**Помните!
от Вашей предусмотрительности, осторожности, осведомленности зависит
Ваша защищенность от возникновения риска несанкционированного доступа
к защищаемой информации с целью осуществления финансовых операций лицами,
не обладающих правом их осуществления!**