Информационная безопасность

В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-П[1] ООО «Цитадель Э.М.» доводит до вашего сведения основные рекомендации по соблюдению информационной безопасности:

- **Обеспечение безопасности компьютера:**
    - Использование только лицензионного программного обеспечения;
    - Регулярное обновление операционных систем и установленного программного обеспечения;
    - Использование антивирусного программного обеспечения и его регулярное обновление;
    - Ограничение доступа к компьютеру посторонних лиц;
    - Использование блокировки компьютера в случае ухода с рабочего места, при завершении работы – выключение компьютера;
    - Обеспечение контроля за действиями специалистов при обслуживании компьютера.
    - Периодически очищать историю посещений сайтов, чистить кэш и cookie. Данная функция встроена во все веб браузеры.
- **Соблюдение правил безопасного использования Интернет:**
    - Ограничение использования сомнительных интернет - ресурсов, сайтов социальных сетей, программ обмена мгновенными сообщениями;
    - Не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скачанные с неизвестных интернет - сайтов, присланные по электронной почте с неизвестных адресов;
    - Не отвечать на подозрительные сообщения, полученные с неизвестных адресов.
- **Пароли:**
    - Использование надежных паролей, содержащих не менее 6 различных символов (сочетание букв/цифр, большого/малого регистра);
    - Не допускается передача паролей, их хранение в открытом виде, в браузерах;
    - Регулярное обновление паролей;
    - Не использовать одинаковые пароли для доступа к различным системам.
    - Не использовать автоматическое сохранение и автозаполнение паролей в веб-браузерах.
- **Контроль подключения:**
    - Не использовать компьютер третьих лиц для подключения к корпоративным сервисам;

[1] «Положение об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (утв. Банком России 17.04.2019 N 684-П)

- Не работать в системе с компьютера, использующего подключение к общедоступной wi-fi сети;

- Необходимо удостовериться в том, что браузер использует безопасное соединение (адресная строка браузера начинается с https, либо используется значок в виде замка);

- Не доверять пароль от корпоративной сети wi-fi третьим лицам.

- **Правила безопасности при использовании ЭЦП:**
    - Не доверять ключи ЭЦП третьим лицам.

    - Не оставлять ключи ЭЦП подключенными к компьютеру, не копировать ЭЦП на компьютер.

    - Должно быть исключено бесконтрольное проникновение и пребывание в помещениях, в которых используются технические средства АРМ посторонних лиц.

При невыполнении или неполном выполнении настоящих требований по обеспечению информационной безопасности клиент принимает на себя риск возможных потерь.