Приложение №1 к приказу №165 от 24.05.19

ЦЕНТР ИНВЕСТИЦИЙ
www.деньгисрочно.рф

Общество с ограниченной ответственностью
Микрокредитная компания «Центр Инвестиций»

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

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

1. 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.

2. Соблюдение правил безопасного использования информационно-телекоммуникационной сети 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.

3. Пароли:

- использование надежных паролей, содержащих не менее 8 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.

4. Ключ электронной подписи (ключ ЭП) и использование СКЗИ:

- хранение в тайне ключа ЭП и обеспечение сохранности ключа ЭП и ключевого носителя;
- применение всех возможных мер для предотвращения потери ключа ЭП, раскрытия, искажения и несанкционированного использования;
- применение только сертифицированной версии СКЗИ «КриптоПро CSP», в том числе при самостоятельном изготовлении ключа ЭП на своем рабочем месте;
- немедленное обращение в Удостоверяющий центр, выпустивший ключ ЭП, с заявлением на прекращение действия сертификата в случае потери, раскрытия, искажения ключа ЭП, в случае, если стало известно, что этот ключ ЭП используется или использовался ранее другими лицами, а также в иных случаях компрометации ключа ЭП или при подозрениях на его компрометацию.

При невыполнении или неполном выполнении настоящих требований по обеспечению информационной безопасности вы принимаете на себя риск осуществления финансовых операций лицами, не обладающими правом на совершение данных операций, а также разглашения информации о финансовых операциях. При утере или разглашении логина и пароля – риск несанкционированного доступа к просмотру документов, содержащих информацию по финансовым операциям, с возможными последующими мошенническими действиями. При утере ключа ЭП – риск несанкционированного доступа к осуществлению финансовых операций.

[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)