Приложение № 4
к Положению об информационной безопасности,
утвержденному приказом от 07.03.2023 № 1
МКК ОРФМСМСП (ФОНД)

Рекомендации
Микрокредитной компании Омский региональный фонд
микрофинансирования субъектов малого и среднего предпринимательства
по защите информации в целях противодействия незаконным финансовым операциям

1. Микрокредитная компания Омский региональный фонд микрофинансирования субъектов малого и среднего предпринимательства (далее – Фонд) уведомляет своих контрагентов, заемщиков, поручителей, залогодателей и представителей указанных лиц, использующих автоматизированные системы для получения, подготовки, обработки, передачи и хранения информации в электронной форме, о **возможных рисках** получения несанкционированного доступа к информации, с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, в том числе при утрате (потере, хищении) контрагентом, заемщиком, поручителем, залогодателем и представителем указанных лиц устройства, с использованием которого им совершались действия в целях осуществления финансовой операции и необходимости защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, своевременному обнаружению воздействия вредоносного кода.

2. В целях предотвращения несанкционированного доступа к информации и нарушения штатного функционирования средства вычислительной техники, Фонд рекомендует следующие **меры защиты**:

2.1. В целях защиты мобильных устройств:

- своевременно устанавливайте обновления безопасности операционной системы;
- при наличии технической возможности включите шифрование данных на своём мобильном устройстве;
- не отключайте и не взламывайте встроенные механизмы безопасности вашего мобильного устройства;
- сохраняйте в тайне Ваши имя пользователя (логин), пароль для доступа в информационные системы и СМС-коды. Не сообщайте эти данные никому;
- учетные записи операционной системы должны быть защищены паролями;
- не храните логин и пароль в мобильном телефоне, смартфоне;
- регулярно производите смену паролей;
- не используйте одинаковые логин и пароль для доступа к различным системам;
- длина пароля должна быть не менее 8 символов;
- в пароле обязательно должны присутствовать заглавные и прописные символы, цифры, а также специальные символы, например, #, %, ^, * и т.д.;
- не используйте функцию запоминания логина и пароля;
- в качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, номер автомобиля, адрес места жительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
- не произносите вслух, не записывайте и не храните пароли в любом доступном посторонним лицам месте.

2.2. В целях защиты персональных компьютеров:

- используйте только лицензионное системное и прикладное программное обеспечение;
- установите на компьютер только одну операционную систему;
- не устанавливайте и не используйте на компьютере программы для удаленного управления, например TeamViewer;

- 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 отключение 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.