



# Новгородский фонд поддержки малого предпринимательства

(микрокредитная компания)

www.ncspr.ru

Россия, 173021, г. Великий Новгород, ул. Кочетова, д. 30

тел./факс: (8162) 67-02-84, 67-00-22

ИНН / КПП: 5321059541 / 532101001

Утверждено Приказом  
Председателя Правления  
Г.Ф. Степанова

№ 19/ПК от «31» мая 2019г.

## Рекомендации по защите информации в целях противодействия незаконным финансовым операциям.

1. Новгородский фонд поддержки малого предпринимательства (микрокредитная компания) в рамках соблюдения требований Положения Банка России от 17.04.2019 № 684-П «Положения 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» уведомляет своих клиентов 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) клиентом 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 Новгородский фонд поддержки малого предпринимательства (микрокредитная компания) рекомендует следующие **меры защиты**:

2.1. В целях защиты мобильных устройств:

- Своевременно устанавливайте обновления безопасности операционной системы;

- 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.