РУССКОЕ КРЕДИТНОЕ ОБЩЕСТВО

Приложение №2
к Приказу №1/2-ю «Об утверждении правил информационных материалов (памятки, рекомендации) для получателей финансовых услуг Общества с ограниченной ответственностью Микрокредитная компания «Русское кредитное общество» от «23» июля 2021 года

РЕКОМЕНДАЦИИ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ МИКРОКРЕДИТНАЯ КОМПАНИЯ «РУССКОЕ КРЕДИТНОЕ ОБЩЕСТВО» ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

В связи с применением лицами, пользующимися услугами (далее – «**Клиенты**») Общества с ограниченной ответственностью Микрокредитная компания «Русское кредитное общество» (далее – «**Общество**») автоматизированных систем для получения, подготовки, обработки, передачи и хранения информации в электронной форме, в том числе информации:

– содержащей персональные данные клиента и иных лиц;

– содержащихся в документах, составляемых при осуществлении финансовых операций и удостоверения права распоряжаться денежными средствами, ценными бумагами или иным имуществом;

– об осуществлённых финансовых операциях;

– ключевой информации средств криптографической защиты информации при осуществлении финансовых операций (криптографические ключи) (далее – «**Информация**»)

Общество предупреждает клиентов о необходимости осуществлять защиту информации в связи с наличием возможных рисков несанкционированного доступа к ней с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и с этой целью рекомендует следующее:

1. ДЛЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ:

(01) Не сообщать посторонним лицам, в том числе в сети «Интернет», персональные данные или информацию о финансовых операциях, о банковских картах (счета), логины и пароли доступов, историю операций, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к защищаемой информации.

(02) Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах (далее – «**Устройство**» или «**Устройства**»), с использованием которых осуществляются финансовые операции.

(03) Не использовать функцию запоминания логина и пароля.

(04) Не использовать одинаковые логин и пароль для доступа к различным системам.

(05) Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имён, номеров телефонов и памятных дат.

(06) Регулярно производить смену паролей.

(07) По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.

(08) Завершать сеанс с электронными сетевыми ресурсами, используя соответствующий пункт меню (например, «Выйти»).

(09) При передаче информации с использованием чужих компьютеров или иных средств доступа, не сохранять на них персональные данные другую информацию, а после завершения всех операций убедиться, что персональные данные и другая информация не сохранились.

(10) Не передавать никакой персональной и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций. Если получение таки писем инициировано не Вами.

(11) Не переходить по ссылкам в таких письмах, не открывать вложенные (такие ресурсы могут содержать вредоносное программное обеспечение).

(12) Не звонить по телефонам, указанным в подобных письмах, и не отвечать на них.

(13) Для связи использовать номера телефонов и электронные адреса, указанные на официальных сайтах владельцев финансовых сервисов.

(14) При регистрации на интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте.

(15) Контролировать конфигурацию устройства, с использованием которого совершаются действия в целях осуществления финансовой операции. Не запускать на своём компьютере, телефоне и/или ином устройстве, содержащем автоматизированную систему, не заслуживающие доверия источников.

(16) Использовать антивирусное программное обеспечение и межсетевые экраны с целью своевременного обнаружения воздействия вредоносного кода.

(17) Регулярно производить обновление системных и прикладных программных средств.

(18) В случае обнаружения подозрительных действий, совершенных в автоматизированной системе устройства незамедлительно сменить логин и пароль и сообщить об этом Обществу (ООО МКК «Русское кредитное общество»).

(19) При утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции-незамедлительно сообщить об этом доступными средствами связи Обществу.

(20) При наличии несанкционированных действий с денежными средствами, иных незаконных финансовых операций-незамедлительно подать заявление о данном факте в правоохранительные органы и сохранить доказательства таких действий в устройстве.

2. ДЛЯ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ПРОГРАММНЫХ КОДОВ, ПРИВОДЯЩИХ К НАРУШЕНИЮ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ВРЕДОНОСНЫЙ КОД), В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ:

(01) В автоматизированной системе устройства Клиента должны применяться только официально приобретённые средства защиты.

(02) Установка и регулярное обновление средств антивирусной защиты должны осуществляться в соответствии с технической документацией.

(03) В целях обеспечения антивирусной защиты производится антивирусный контроль системы Устройства.

(04) Обязательному антивирусному контролю подлежит вся информация.

(05) К применению допускаются только лицензионные антивирусные средства.

(06) При работе с иными носителями информации необходимо перед началом работы осуществить и проверку на предмет отсутствия компьютерных вирусов.

(07) Защита от вирусов состоит из нескольких этапов.

– На первом этапе выполняются регулярные профилактические работы по выявлению вирусов.

– На втором этапе производится анализ ситуации проявления вируса (вирусов) и причины появления.

– На третьем этапе выполняется уничтожение вируса (вирусов) из автоматизированной системы Устройства.

(08) Ярлык для запуска антивирусной программы должен быть вынесен на основной экран Устройства.

(09) Обновление антивирусных пакетов осуществляется на постоянной основе.

(10) Клиент должен осуществлять регулярный контроль работоспособности антивирусных программ, обеспечить невозможность самовольного, либо несанкционированного отключения средств антивирусной защиты.

(11) Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

(12) Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.

(13) Лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их раздельную установку в автоматизированной системе, почтовых ресурсах и межсетевых экранах.

(14) Антивирусная программа должна обеспечить сохранение безопасного состояния автоматизированной системы при своих сбоях.