«УТВЕРЖДЕНО»
приказом № 06/ЗИ от «07» июня 2019 года
Генрального директора ООО " Рич"

Вступает в силу с «01» июля 2019 года

Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

При использовании систем дистанционного финансового обслуживания и несоблюдении рекомендаций, указываемых в правилах безопасности таких систем, для пользователя возможны риски получения несанкционированного доступа (далее – НСД) к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, утечки персональных данных и иной защищаемой информации.

В целях предотвращения возможных негативных последствий вследствие реализации таких рисков рекомендуется:

1. Не сообщать посторонним лицам персональные данные или информацию о банковских картах (счетах) через сеть Интернет, логины и пароли доступов, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Вашей защищаемой информации.
2. Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции.
3. Не использовать функцию запоминания логина и пароля в браузерах для используемых платежных систем.
4. Не использовать одинаковые логин и пароль для доступа к различным системам.
5. Регулярно производить смену паролей. Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имен, номеров телефонов и памятных дат.
6. По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.
7. Завершать сеанс работы с платежными системами, используя соответствующий пункт меню (например, «Выйти»).

8. При выполнении операций в платежных системах с использованием чужих компьютеров или иных средств доступа не сохранять на них персональные данные и другую информацию, а после завершения всех операций убедиться, что персональные данные и другая информация не сохранились.
9. Не передавать никакой персональной 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 переходить по ссылкам в таких письмах, не открывать вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение). Не звонить по телефонам, указанным в подобных письмах, и не отвечать на них. Для связи использовать номера телефонов и электронные адреса, указанные на официальных сайтах владельцев финансовых сервисов.
10. При регистрации на сторонних интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте.
11. Не запускать на своем компьютере программы, полученные из незаслуживающих доверия источников.
12. Использовать антивирусное программное обеспечение и межсетевые экраны.
13. Регулярно производить обновление системных и прикладных программных средств.
14. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно сменить логин и пароль и сообщить об инциденте информационной безопасности в Службу технической поддержки Банка или платежного сервиса.
15. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, утраты (потери, хищения) устройства, с использованием которого осуществлялись финансовые операции, подать заявление на временное отключение от платежной системы, подать заявление о данном факте в правоохранительные органы и прекратить использование (обесточить) персонального компьютера и иных средств доступа в целях сохранения доказательной базы.