

Рекомендации по защите информации от воздействия вредоносных кодов в целях противодействия незаконным финансовым операциям

В связи с применением лицами, пользующимися услугами ООО «УК ПРОМСВЯЗЬ» (далее соответственно – клиенты, Общество), автоматизированных систем для получения, подготовки, обработки, передачи и хранения в электронной форме информации (далее соответственно - автоматизированные системы, защищаемая информация):

- содержащей персональные данные клиента;
- содержащейся в документах, составляемых при осуществлении финансовых операций;
- об осуществленных финансовых операциях,

Общество, в рамках соблюдения требований 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 (утв. Банком России 17.04.2019 № 684-П), предупреждает клиентов о необходимости осуществлять защиту указанной информации в связи с наличием возможных рисков получения 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, контроля конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции:

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

1.2. Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции.

1.3. Не использовать функцию запоминания логина и пароля.

1.4. Не использовать одинаковые логин и пароль для доступа к различным системам.

1.5. Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имен, номеров телефонов и памятных дат.

1.6. Регулярно производить смену паролей.

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

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

1.9. При передаче информации 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.

1.10. Не передавать никакой персональной и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами.

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

- 1.12. Не звонить по телефонам, указанным в подобных письмах, и не отвечать на них.
- 1.13. Для связи использовать номера телефонов и электронные адреса, указанные на официальных сайтах владельцев финансовых сервисов.
- 1.14. При регистрации на интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте.
- 1.15. Контролировать конфигурацию устройства, с использованием которого совершаются действия в целях осуществления финансовой операции. Не запускать на своем компьютере, телефоне и/или ином устройстве, содержащем автоматизированную систему, не заслуживающих доверия источников.
- 1.16. Использовать антивирусное программное обеспечение и межсетевые экраны с целью своевременного обнаружения воздействия вредоносного кода
- 1.17. Регулярно производить обновление системных и прикладных программных средств.
- 1.18. В случае обнаружения подозрительных действий, совершенных в автоматизированной системе устройства, незамедлительно сменить логин и пароль и сообщить об этом в Общество.
- 1.19. При утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции – незамедлительно сообщить об этом доступными средствами связи в Общество.
- 1.20. 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), своевременного обнаружения воздействия вредоносного кода в целях противодействия незаконным финансовым операциям:

- 2.1. В автоматизированной системе устройства Клиента должны применяться только официально приобретенные средства антивирусной защиты.
- 2.2. Установка и регулярное обновление средств антивирусной защиты должны осуществляться в соответствии с технической документацией.
- 2.3. В целях обеспечения антивирусной защиты производится антивирусный контроль автоматизированной системы Устройства.
- 2.4. Обязательному антивирусному контролю подлежит вся информация.
- 2.5. К применению допускаются только лицензионные антивирусные средства.
- 2.6. При работе с иными носителями информации необходимо перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
- 2.7. 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.
- 2.8. Ярлык для запуска антивирусной программы должен быть вынесен на основной экран Устройства.
- 2.9. Обновление антивирусных пакетов осуществляется на постоянной основе.
- 2.10. Клиент должен осуществлять регулярный контроль работоспособности антивирусных программ, обеспечить невозможность самовольного, либо несанкционированного отключения средств антивирусной защиты.

- 2.11. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
- 2.12. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.
- 2.13. Лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их отдельную установку в автоматизированной системе, почтовых ресурсах и межсетевых экранах.
- 2.14. Антивирусная программа должна обеспечивать сохранение безопасного состояния автоматизированной системы при своих сбоях.