Утверждено приказом генерального директора
АО «ТРИНФИКО»
№ ТРФ-103/220202/0-001 от 30.12.2021
Т.В. Рудницкая

**Рекомендации АО «ТРИНФИКО» по защите информации в целях противодействия незаконным финансовым операциям**

Настоящие рекомендации по защите информации в целях противодействия незаконным финансовым операциям разработаны АО «ТРИНФИКО»,[1] (далее - Компания), в соответствии с требованиями Положения Банка России от 20.04.2021 № 757-П «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» и направлены на защиту информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

**1. Информация о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.**

В результате неправомерных действий третьих лиц информация, связанная с проведением финансовых операций, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах в рамках обслуживания, содержащаяся в электронных документах, которыми обмениваются клиенты с Компанией (электронные сообщения), информация, необходимая для авторизации клиента и удостоверения его прав на распоряжение имуществом (ключи, логины, пароли, СМС подтверждения и т.п.), информация о фактически осуществленных финансовых операциях, а также ключевая информация применяемых средств криптографической защиты (криптографические ключи) (далее по отдельности и совместно именуется – защищаемая информация), может быть подвергнута воздействию вредоносных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники.

Клиенты Компании несут риски негативных последствий вследствие обстоятельств:

- получение третьими лицами несанкционированного доступа к персональным данным и иной значимой защищаемой информации конфиденциального характера, а также их разглашение;
- утрата, потеря (хищение) идентификаторов доступа клиента (в случае их применения), с использованием которых осуществляются финансовые операции;
- совершение злоумышленниками юридически значимых действий: операций с имуществом, подключения и отключения услуг (в том числе платных), внесение изменений в регистрационные данные, использование счетов клиентов и находящегося на них имущества для прикрытия каких-либо действий, носящих противоправный характер, и совершение иных действий против воли клиента;
- деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения клиентами или Компанией своих обязательств по договору или невозможности использования сервисов Компании для реализации намерений клиентов;
- разглашение относящейся к клиенту информации конфиденциального характера: сведений об операциях, имуществе, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации;
- совершение в отношении клиента иных противоправных действий, связанных с информационной безопасностью.

2. **Информация о мерах по предотвращению несанкционированного доступа к защищаемой информации**.

В целях предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, для контроля конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременного обнаружения воздействия вредоносного кода рекомендуем принимать следующие меры:

[1] Лицензия профессионального участника рынка ценных бумаг на осуществление деятельности по управлению ценными бумагами № 177-06326-001000 от 16 сентября 2003 года; Лицензия профессионального участника рынка ценных бумаг на осуществление брокерской деятельности № 177-06305-100000 от 16 сентября 2003 года; Лицензия профессионального участника рынка ценных бумаг на осуществление дилерской деятельности № 177-06323-010000 от 16 сентября 2003 года; Лицензия профессионального участника рынка ценных бумаг на осуществление депозитарной деятельности № 177-06362-000100 от 19 сентября 2003 года.

1) использовать и хранить устройство таким образом, чтобы исключить возможность его хищения и несанкционированного использования;

2) использовать современные и актуальные методы блокировки устройств (TouchID, FaceID, ПИН-КОД И др.);

3) устанавливать надежные пароли и не использовать один пароль ко всем системам, регулярно менять пароли, хранить пароли в тайне от всех лиц, без исключения;

4) обязательное блокирование устройства;

5) при утрате (потере, хищении) устройства позаботиться о смене паролей доступа к системам;

6) проверять реквизиты и не сообщать третьим лицам информацию, полученную для проведения финансовой операции в СМС-сообщениях;

7) использовать только лицензионное программное обеспечение;

8) выполнять правила, требования, положения, установленные эксплуатационной документацией на программное обеспечение, информационную систему (ресурс), средства защиты информации, включая средства электронной подписи, используемые при обмене информацией;

9) настроить автоматическое обновление программного обеспечения;

10) устанавливать приложения, скачанные только с официальных магазинов приложений (App Store или Google Play) или с сайтов производителей;

11) использовать антивирусное программное обеспечение и встроенные средства межсетевого экранирования (брандмауэр);

12) настроить автоматическую полную проверку устройств на предмет наличия вирусов и вредоносного программного кода не реже одного раза в месяц;

13) при возникновении подозрения на наличие вируса (признаки - значительное замедление работы, увеличение исходящего/входящего трафика, нетипичная работа устройства, частое появление сообщений о системных ошибках и сбоях и т.п.) провести дополнительные проверки и приостановить работу с финансовой информацией до устранения проблем;

14) не посещать неофициальные и подозрительные Интернет-ресурсы, а также не использовать неофициальные и подозрительные мобильные приложения;

15) использовать для хранения ключей электронной подписи внешние носители. Настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например, e-token, смарт-карта и т.п.;

16) крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы;

17) не разглашать посредством средств связи (по телефону или электронной почте) информацию, которая может повлечь несанкционированный доступ к системам, конфиденциальной информации или финансовым операциям;

18) не использовать подключение к публичным сетям связи (WiFi) для осуществления финансовых операций или передачи конфиденциальной информации;

19) соблюдать принцип разумного раскрытия идентификационных данных, в том числе персональных данных (в случае запроса у клиента указанной информации в связи с оказанием услуг Компанией, клиенту рекомендуется по возможности оценить ситуацию и уточнить полномочия запрашивающего лица и процедуру предоставления запрашиваемой информации через независимый канал связи);

20) при подозрении в несанкционированном обращении третьего лица от имени клиента для получения услуг Компании, клиенту необходимо незамедлительно обратиться в Компанию;

21) осуществлять звонки и направлять почтовые сообщения (в том числе электронные) в Компанию только по номеру телефона, почтовому и электронному адресу, указанным на сайте Компании в информационно-телекоммуникационной сети Интернет по адресу: https://www.trinfico.ru/ (от лица Компании не могут поступать звонки или сообщения, в которых от клиента требуют предоставить идентификаторы доступа).

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к личному кабинету и электронной почте клиента несет клиент. Клиент безусловно несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

Настоящие рекомендации подлежат доведению до сведения клиентов путем размещения на официальном сайте Компании в информационно-телекоммуникационной сети Интернет по адресу: https://www.trinfico.ru/