Рекомендации по соблюдению информационной безопасности клиентами Акционерного общества «Национальная товарная биржа» (АО НТБ) в целях противодействия незаконным финансовым операциям

г. Москва, 2023 г.

1. Общие положения.

В соответствии с требованиями Положения Банка России от 20.04.2021 N 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" Акционерное общества «Национальная товарная биржа» (АО НТБ) (далее по тексту - Общество) доводит до Вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017) не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации. В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, регламентах, правилах и иных документах Общества, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

2. Общие рекомендации.

В целях снижения риска реализации инцидентов информационной безопасности (ГОСТ Р 57580.1-2017) – нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов Общества и (или) нарушению конфиденциальности, целостности и доступности информации вследствие:

- несанкционированного доступа к Вашей информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых);
- потери (хищения) носителей ключей электронной подписи, с использованием которых осуществляются критичные (финансовые) операции;
- воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;
- совершения в отношении Вас иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в т.ч. автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов (ГОСТ Р 57580.1-2017) Общества. Внимательно изучите договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомьтесь с разделами, посвященными информационной безопасности/конфиденциальности.

3. Риск получения третьими лицами несанкционированного доступа к защищаемой информации

При осуществлении критичных (финансовых) операций следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления. Такие риски могут быть обусловлены включая, но не ограничиваясь следующими примерами:

• кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода; и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;

• установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от Вашего имени;

• использование злоумышленником утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит ему обойти защиту;

• кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам Общества с этого устройства;

• получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

• перехват электронных сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Обществом. Или в случае получения доступа к вашей электронной почте отправка сообщений от Вашего имени в Общество.

4. Снижение риска финансовых потерь

A. Обеспечьте защиту устройства, с которого Вы пользуетесь услугами Общества. К таким мерам включая, но не ограничиваясь могут быть отнесены:

• использование только лицензионного программного обеспечения, полученного из доверенных источников;

• запрет на установку программ из непроверенных источников;

• наличие средств защиты таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;

• настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;

• хранение, использование устройства с целью избежать рисков кражи и/или утери;

• своевременное обновление операционной системы, особенно в части обновлений безопасности. Имейте в виду, что обновления снижают риски заражения вредоносным кодом. Злоумышленники часто используют старые уязвимости;

• активация парольной или иной защиты для доступа к устройству.

B. Обеспечьте конфиденциальность:

• храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Общества: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае вероятной компрометации немедленно примите меры для их смены и/или блокировки;

• соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах в случае, если у Вас запрашивают указанную информацию в привязке к сервисам Общества по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон Общества.

C. Проявляйте осторожность и предусмотрительность:

• будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам

через электронную почту или интернет-ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;

• внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Общество или его уполномоченных/доверенных лиц;

• будьте осторожны при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;

• будьте осторожны с файлами из новых или «недоверенных» источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);

• не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

• следите за информацией в прессе и на сайте Общества о последних критичных уязвимостях и о вредоносном коде;

• при подаче поручений и/или ином обращении в Общество, осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Общества. И имейте в виду, что от лица Общества не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д. Кодовое слово может быть запрошено только, если Вы сами позвонили в Общество;

• имейте в виду, что, если Вы передаете Ваш телефон и/или иное устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к сервисам и системам Общества, которыми пользовались Вы. В связи с этим, при утере, краже телефона (SIM карты), используемого для получения СМС кодов или доступа к системам и(или) сервисам Общества с Мобильного приложения:

(1) незамедлительно проинформируйте Общество;

(2) по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокируйте и перевыпустите SIM-карту, а также смените пароли и коды доступа (кодовые слова) к сервисам и/или системам Общества;

• при подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и\или заблокировать доступ, обратившись в Общество, в отношении ключевой информации, если это применимо для вашей услуги – отозвать скомпрометированный ключ электронной подписи/шифрования в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора.

D. При работе с ключами электронной подписи необходимо:

• 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.;

• 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;

• использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли в открытом виде на компьютере/мобильном устройстве.

E. При работе на компьютере необходимо:

• использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);

• своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);

• использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;

• использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;

• использовать сложные пароли;

• ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

F. При работе с Мобильного устройства необходимо:

• не оставлять свое Мобильное устройство без присмотра чтобы исключить его несанкционированное использование;

• использовать только официальные Мобильные приложения;

• не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;

• установить на Мобильном устройстве пароль для доступа к устройству.

G. При обмене информацией через сеть Интернет необходимо:

• не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;

• не вводить персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;

• ограничить посещения сайтов сомнительного содержания;

• не сохранять пароли в памяти интернет-браузера если к компьютеру есть доступ у третьих лиц

• не кликать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;

• не открывать файлы, полученные (скачанные) из неизвестных источников.

При подозрении в компрометации ключей электронной подписи/шифрования или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно обращаться в Общество.