



**ITI
CAPITAL**

Приложение № 1

УТВЕРЖДЕНО
Приказом Председателя Правления
АО «ИК «Ай Ти Инвест»
от « 10 » января 2022 г. № 22-10/01-2

**Рекомендации по соблюдению информационной безопасности клиентами
АО «ИК «Ай Ти Инвест» в целях противодействия
незаконным финансовым операциям
Версия 1.0.**

г. Москва, 2022 г.

Содержание

1. Общие положения.....	3
2. Общие рекомендации.....	3
3. Риск получения третьими лицами несанкционированного доступа к защищаемой информации.....	3
4. Снижение риска финансовых потерь.....	4

1. Общие положения

1.1. В соответствии с требованиями Положения Банка России от 20.04.2021 г. № 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» АО «ИК «Ай Ти Инвест» (далее – Общество) доводит до Вашего сведения настоящие «Рекомендации по соблюдению информационной безопасности клиентами АО «ИК «Ай Ти Инвест» в целях противодействия незаконным финансовым операциям» (далее – Рекомендации).

1.2. Настоящие Рекомендации содержат 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.

1.3. 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 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.

1.4. В связи с тем, что требования информационной безопасности также могут быть отражены во внутренних документах Общества, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов Общества.

2. Общие рекомендации

2.1. В целях снижения риска реализации инцидентов информационной безопасности («ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», далее – 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 том числе 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.

2.2. Рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в том числе автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов (ГОСТ Р 57580.1-2017) Общества. Внимательно изучите договор, заключаемый с Обществом, 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

3.1. 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 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

4.1. 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.

4.2. 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.

4.3. 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 том числе 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, заключенному с Обществом, 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 могут 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:
 - Незамедлительно проинформируйте Общество;
 - 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, заключаемом с Обществом, приложениях к договору и иных документах, связанных с исполнением договора.
- 4.4. 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.
- 4.5. 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.
- 4.6. 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 СМС-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;
 - Установить на мобильном устройстве пароль для доступа к устройству.
- 4.7. При обмене информацией через информационно-телекоммуникационную сеть «Интернет» необходимо:
- Не открывать электронные письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких электронных 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 информационно-телекоммуникационной 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.

Председатель Правления



М.А. Панкова



Прошито, пронумеровано
скреплено печатью

Meliss

Председатель Правления
ООО «ИК «Ай Ти Инвест»
Иванова М. Анная



[Handwritten signature]