УТВЕРЖДЕНЫ
Приказом Генерального директора
№13-25/ДИБ/УКД от «20» мая 2025г.

РЕКОМЕНДАЦИИ
по соблюдению информационной безопасности клиентами в целях противодействия незаконным финансовым операциям

ООО «УК «ДОХОДЪ»

Санкт-Петербург
2025г.

1. Общие положения

1.1. Настоящие Рекомендации по соблюдению информационной безопасности клиентами в целях противодействия незаконным финансовым операциям (далее — Рекомендации) разработаны 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".

1.2. ООО «УК «ДОХОДЪ» (далее — 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.

1.3. Рекомендации по соблюдению информационной безопасности так же 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.

1.4. В Рекомендациях Общество обращает Ваше внимание с целью снижения риска реализации инцидентов информационной безопасности на нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов Общества и/или нарушить конфиденциальность, целостность и доступность информации, вследствие:

- несанкционированного доступа к вашей информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- утраты (потери, хищении) клиентом устройства или контроля за конфигурацией устройства, с использованием которого им совершались действия в целях осуществления финансовой операции;
- несвоевременного обнаружения воздействия вредоносного кода на устройство, с которого совершаются критичные (финансовые) операции;
- совершения в отношении Вас иных противоправных действий, связанных с информационной безопасностью.

2. Рекомендации

2.1. Общество рекомендует соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании информационных систем Общества.

2.2. Перед тем как начнете использовать информационные системы Общества, внимательно изучите договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомьтесь с разделами, посвященными информационной безопасности/конфиденциальности.

2.3. При осуществлении критичных (финансовых) операций следует принимать во внимание риск получения третьми 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:

2.3.1. 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.

2.3.2. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от Вашего имени.

2.3.3. Использование злоумышленниками утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты от несанкционированных финансовых операций, что позволит им обойти защиту.

2.3.4. 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.

2.3.5. 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.

2.3.6. 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.

2.4. Для снижения риска финансовых потерь:

2.4.1. 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 средства защиты таких как: антивирусное программное обеспечение с регулярно и своевременно обновляемыми базами, персональный межсетевой экран;
- хранение и использование устройства с целью избежать рисков кражи и/или утери;
- своевременное обновление операционной системы, особенно в части обновлений безопасности. Своевременное обновление снижает риски заражения устройства вредоносным кодом — злоумышленники часто используют старые уязвимости;
- активация парольной или иной защиты для доступа к устройству.

2.4.2. Обеспечьте конфиденциальность:

- храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученную от Общества: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для 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 официальный телефон контактного центра Общества.

2.4.3. 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 иных 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 программным обеспечением 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 наличии в рамках Вашего продукта сервиса контакт центра осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Общества. Имейте ввиду, 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 контакт центр;

- к Вашему сведению, если Вы передаете свой телефон и/или устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери своего устройства злоумышленники могут воспользоваться им для доступа к системам Общества, которыми пользовались Вы. В связи с этим при утере, краже телефона (SIM-карты), используемого для получения СМС-кодов или доступа к системам Общества с Мобильного приложения: 1) незамедлительно проинформируйте Общество через контактный центр; 2) заблокируйте и перевыпустите SIM-карту; 3) смените пароль в Мобильном приложении;

- при подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать доступ, обратившись в Общество;

- помните, что наличие «эталонной» резевной копии может облегчить и ускорить восстановление Вашего устройства;

- для финансовых операций лучше всего использовать отдельное, максимально защищенное устройство, доступ к которому есть только у Вас;

- контролируйте свой телефон, используемый для получения СМС-кодов. В случае выхода из строя SIM-карты незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.

2.4.4. При работе с ключами электронной подписи необходимо:

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

- внимательно относится к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они 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.

2.4.5. 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.

2.4.6. При работе с Мобильным приложением необходимо:

- не оставлять свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование Мобильного приложения;
- использовать только официальные Мобильные приложения, скачанные и установленные из доверенных источников;
- не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в СМС-сообщении, Push-уведомлении или по электронной почте, в том числе от имении Общества;
- установить на мобильном устройстве пароль для доступа к нему и приложению.

2.4.7. 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 ресурсах;
- ограничивать посещения сайтов сомнительного содержания;
- не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;
- не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
- не открывать файлы, полученные (скачанные) из неизвестных источников.

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