УТВЕРЖДЕНО

Приказом Генерального директора

ООО «Диалог Инвестиции»

№ 13/2023 от «22» мая 2023 г.

Рекомендации клиентам Общества с ограниченной ответственностью «Диалог Инвестиции» по соблюдению мер информационной безопасности в целях предотвращения несанкционированного доступа к защищаемой информации и противодействия незаконным финансовым операциям

г. Москва
2023 год

1. Общие положения

1.1. 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» Общество с ограниченной ответственностью «Диалог Инвестиции» (далее по тексту – Общество) доводит до сведения своих клиентов Рекомендации по соблюдению мер информационной безопасности в целях предотвращения несанкционированного доступа к защищаемой информации и противодействия незаконным финансовым операциям, а именно:

а) информацию о возможных рисках несанкционированного доступа к защищаемой информации, с целью совершения финансовых операций лицами, не обладающими правом их совершения;

в) информацию о рекомендуемых мерах по предотвращению 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, контролю конфигурации устройства, с использованием которого клиентом совершаются финансовые операции;

б) рекомендации по своевременному обнаружению вредоносных программ и кодов и по обеспечению защиты информации от их воздействия, приводящих к нарушению штатного функционирования аппаратных и программных средств, в целях противодействия незаконным финансовым операциям, совершаемым третьими лицами.

1.2. Настоящие рекомендации по соблюдению клиентами Общества информационной безопасности - совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения данных мер защиты, не гарантируют полного обеспечения конфиденциальности, целостности и доступности информации, но позволяют в целом повысить уровень информационной безопасности и минимизировать негативные последствия при возникновении нежелательных событий.

1.3. Для обеспечения надлежащей степени защиты информации необходимо использовать комплексный подход, при котором вопросам информационной безопасности уделяется достаточно внимания не только Обществом, но и клиентами Общества.

Применение клиентами Общества рекомендуемых мер по соблюдению информационной безопасности позволит получить максимальное предотвращение совершения несанкционированных действий со стороны злоумышленников и обеспечить минимальный размер ущерба в результате совершения таких действий.

1.4. В связи с тем, что требования по соблюдению клиентами Общества мер информационной безопасности также могут быть указаны в договорах, и иных внутренних документах Общества, регламентирующих предоставление клиентам различных финансовых услуг и сервисов, настоящие рекомендации действуют в части, не противоречащей положениям и условиям, указанным в договорах и во внутренних документах Общества.

2. Возможные риски несанкционированного доступа к защищаемой информации.

2.1. Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой разглашение конфиденциальной информации, содержащей ваши персональные данные, сведения о совершенных операциях, а также другие сведения конфиденциального характера.

2.2. Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими лицами юридически значимых действий, включая, но, не ограничиваясь, изменением ваших регистрационных данных, совершением финансовых операций от вашего имени, и совершением иных действий без вашего разрешения, направленных против ваших интересов.

2.3. При осуществлении различных финансовых операций следует принимать во внимание возможные риски получения несанкционированного доступа к защищаемой

информации с целью осуществления незаконных финансовых операций лицами, не обладающими правами на их осуществление.

Такие риски могут быть реализованы включая, но не ограничиваясь, следующими способами:

а) использованием злоумышленниками вашего утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Управляющей компанией в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту;

б) кражей или незаконным доступом злоумышленниками к вашим техническим устройствам, в том числе: к компьютеру, ноутбуку, планшету, мобильному телефону, с помощью которых вы получаете доступ к услугам или сервисам, предоставляемым Обществом, что может повлечь за собой получение этими лицами нежелательного доступа к вашей защищаемой информации и совершение незаконных финансовых операций;

в) кражей пароля и идентификатора доступа или иных ваших 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;

г) получением пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих ваших 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;

д) установкой на ваше техническое устройство вредоносного кода (компьютерного вируса), который позволит злоумышленникам осуществлять финансовые операции от вашего имени, а также получить доступ к вашим логинам, паролям и иным персональным данным;

е) перехватом электронных сообщений и получением 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 в ашего имени в Общество;

ж) совершением злоумышленниками мошеннических действий от имени различных финансовых организаций, в том числе путем телефонных звонков, почтовых рассылок, размещения в сети Интернет ложных (поддельных) ресурсов и ссылок на них, с целью получения конфиденциальных сведений о ваших персональных данных, логинах, паролях, номеров телефонов, адресов электронной почты, сведений о доступе к управлению банковскими счетами, счетами депо, лицевыми счетами в реестрах владельцев ценных бумаг, а также других сведений конфиденциального характера.

3. Рекомендации клиентам по предотвращению несанкционированного доступа к информации и техническим устройствам, используемым для совершения финансовых операций.

В целях снижения риска реализации инцидентов информационной безопасности - нежелательных или неожиданных событий защиты информации, которые могут привести к нарушениям выполнения бизнес-процессов и технологических процессов, как у клиента, так и у Общества, и/или нарушить целостность и конфиденциальность информации по причине:

- несанкционированного доступа к вашему техническому устройству и вашей личной информации лицами, не обладающими правом доступа и осуществления значимых (критичных) операций, в том числе финансовых операций;
- потери (хищения) носителей ключей электронной подписи, с использованием которых, вами осуществляются критичные (финансовые) операции;
- воздействия вредоносного кода на технические устройства, с которых вы можете совершать критичные (финансовые) операции;

- совершения в отношении вас иных противоправных действий, связанных с информационной безопасностью;

Общество рекомендует своим клиентам соблюдать комплекс профилактических действий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации, а также использовать различные меры, позволяющие снизить риски несанкционированного доступа к техническим устройствам и к защищаемой информации, а также снизить риски получения финансовых потерь, включая, но не ограничиваясь следующими мерами:

1) уделяйте особое внимание работе с ключами, паролями, электронными подписями и иной личной информацией, обеспечивайте их сохранность и конфиденциальность;

2) храните в тайне идентификационные личные данные, полученные от Управляющей компании пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае их компрометации немедленно примите меры для их замены и/или блокировки;

3) используйте сложные пароли для входа на свое устройство и для доступа к ключам электронной подписи/ключевым носителям, длинной не менее 8 символов, состоящие из сочетания строчных и прописных букв, цифр и символов;

4) не используйте логины и пароли, установленные ранее для работы с любыми другими программами, сайтами и социальными сетями;

5) не храните свои пароли в открытом доступе, в компьютере/мобильном устройстве, не пересылайте свои пароли по почте, в СМС или иным подобным образом;

6) меняйте регулярно свои пароли на всех устройствах и программах, в том числе на серверах и сетевом оборудовании;

7) соблюдайте принцип разумного раскрытия информации другим лицам о номерах ваших счетов, паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах, а в случае. если у вас запрашивают указанную информацию в привязке к желаемому сервису, по возможности оцените ситуацию и уточните полномочия лица, спрашивающего данную информацию, а также уточните процедуру получения желаемого сервиса через независимый канал связи, например, через контактный телефон или адрес электронной почты Управляющей компании;

8) используйте для хранения ключей электронной подписи внешние носители, при этом настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п.;

9) относитесь внимательно к ключевому носителю, не оставляйте его без присмотра и не передавайте его третьим лицам, извлекайте ключевые носители из компьютера, если они не используются для работы;

10) при подозрении в компрометации ключей электронной подписи/шифрования или в несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов с использованием сервисов Общества следует незамедлительно обратиться в Общество;

11) при подозрении на совершение неизвестными лицами несанкционированного доступа и/или на компрометацию технического устройства следует сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество, в отношении ключевой информации, если это уместно 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 такого договора;

12) используйте для совершения финансовых операций отдельное, максимально защищенное техническое устройство, доступ к которому есть только у вас или у ваших доверенных лиц;

13) ограничьте несанкционированный доступ третьих лиц к Вашему устройству и к специальному программному обеспечению путем установки на нем пароля и настройки персональных прав доступа;

14) не сохраняйте пароли в памяти интернет-браузера, если к вашему компьютеру есть доступ у третьих лиц; а также исключите возможность дистанционного подключения к вашему техническому устройству третьими лицами;

15) не оставляйте без присмотра и обеспечивайте надлежащий контроль за хранением и использованием технического устройства, с которого вы совершаете свои финансовые операции, во избежание возможности его кражи и/или несанкционированного использования;

16) приобретайте только сертифицированные технические устройства у официальных дилеров и(или) в проверенных торговых компаниях и используйте на своих технических устройствах только лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.) и официальные мобильные приложения;

17) не используйте технические устройства, на которых вы совершаете финансовые операции, для обмена сообщениями или файлами с другими лицами с помощью различных сервисов и программ;

18) не совершайте финансовые операции на технических устройствах, которые вы используете также для доступа или работы с развлекательными сайтами (игровые сайты, сайты знакомств, социальные сети, сайты распространения программного обеспечения, музыки, фильмов и т.п.);

19) при работе с мобильным телефоном установите на нем пароль доступа к устройству и к приложениям, используемым вами для совершения финансовых операций, используйте только официальные мобильные приложения, не переходите по неизвестны вам ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте;

20) контролируйте свой мобильный телефон, используемый для получения SMS-сообщений, содержащих коды доступа. В случае выхода из строя SIM карты, незамедлительно обращайтесь к своему сотовому оператору для уточнения причин возникновения такой ситуации, а также для установления сроков получения новой SIM карты и восстановления мобильной связи;

21) при работе с электронной почтой внимательно проверяйте адресата, от которого вам приходят электронные письма. не открывайте письма и вложения в них, полученные от неизвестных отправителей или, в случае наличия сомнений в их подлинности, не переходите по содержащимся в таких письмах ссылкам. Входящие электронные письма могут приходить от злоумышленников, которые маскируются под представителей Общества или иных доверенных лиц Общества;

22) при работе в сети Интернет не посещайте сайты сомнительного содержания, не вводите свою персональную информацию на подозрительных и сомнительных сайтах, а также на неизвестных вам интернет – ресурсах;

23) не совершайте финансовые операции на своем техническом устройстве через открытые публичные и не проверенные сети WI-FI (в кафе, отелях, магазинах, торговых центрах, парках, вокзалах, аэропортах, метро и в общественном транспорте);

24) для оперативного взаимодействия с Обществом используйте только номер телефона и адрес электронной почты, указанные в договоре или на официальном сайте Общества. Помните, что из Общества к вам не могут поступать звонки, письма или сообщения, в которых от вас требуют сообщить СМС-код, пароль, номер карты, кодовое слово и т.д. Кодовое слово может быть запрошено представителем Общества исключительно в целях Вашей идентификации как клиента, и только, если Вы сами первый позвоните в Общество.

4. Рекомендации клиентам по защите информации и технических устройств от воздействия вредоносных программ и кодов, в целях противодействия незаконным финансовым операциям, совершаемым третьими лицами.

В целях защиты технического устройства, специального программного обеспечения и конфиденциальной информации от воздействия на них вредоносных программ и кодов (компьютерных вирусов) Общество рекомендует своим клиентам проявлять должную осторожность и предусмотрительность при использования своего устройства, с помощью которого осуществляются финансовые операции, и применять различные защитные меры, включая, но не ограничиваясь следующими мерами:

1) будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом, который при

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

2) будьте осторожны при просмотре/работе с интернет-сайтами сомнительного содержания, так как вредоносный код может быть загружен с таких сайтов, не нажимайте на баннеры и всплывающие окна, возникающие во время работы на сайтах в сети Интернет;

3) будьте осторожны с файлами из новых или «недостоверных» источников (в том числе архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным программным обеспечением в автоматическом режиме), не открывайте файлы, полученные или скачанные из неизвестных источников;

4) не заходите в системы удаленного доступа с недостоверных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа, а также способный изменить вашу финансовую операцию;

5) установите и своевременно обновляйте на своем техническом устройстве лицензионное антивирусное программное обеспечение с функцией регулярного автоматического сканирования файлов и программ, имеющихся на техническом устройстве. а также обновления вирусных баз и программ для борьбы с компьютерными вирусами;

6) используйте специализированные программы для защиты информации, сохраняемой на техническом устройстве (персональные межсетевые экраны и средства защиты от несанкционированного доступа), а также средства контроля конфигурации технических устройств;

7) подвергайте предварительному антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование внешних носителей информации должно осуществляться в автоматическом режиме;

8) следите за информацией в прессе и на сайте Общества о последних критичных уязвимостях программного обеспечения, предоставляемого Обществом, своевременно загружайте и устанавливайте критические обновления операционной системы, системы безопасности и специального программного обеспечения, используемого для выполнения вами финансовых операций. Такие обновления снижают риски заражения технического устройства вредоносным кодом, т.к. злоумышленники часто используют старые уязвимости в операционных системах и программном обеспечении;

9) установите на используемом вами техническом устройстве по умолчанию максимальный уровень безопасности, не требующий действий пользователя при обнаружении вирусов, чтобы лечение или удаление зараженных файлов выполнялось антивирусным средством в автоматическом режиме;

10) регулярно делайте резервное копирование и сохранение важных для вас данных и информации на используемом вами техническом устройстве. Помните, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление работоспособности вашего технического устройства;

11) не передавайте ваш мобильный телефон и/или компьютер другим неизвестным пользователям, так как они могу установить на него вредоносный код, и в случае кражи или утери данного устройства злоумышленники могут воспользоваться этим вредоносным кодом для доступа к программам и системам, которыми вы пользовались на данных устройствах для совершения финансовых операций.

При утере или краже мобильного телефона (SIM карты), используемого для получения СМС кодов или паролей доступа к программам, предоставляемым Обществом для используемого вами мобильного приложения, вам следует:

- незамедлительно проинформировать о данном факте Общество;
- оперативно, с учетом прочих рисков и особенностей использования вашего мобильного телефона, заблокировать старую SIM карту и оформить новую SIM карту, а также сменить пароль входа в ваше мобильное приложение;

12) при возникновении подозрений на наличие на используемом вами техническом устройстве вредоносного кода необходимо приостановить работу на этом устройстве

провести дополнительные проверки на предмет выявления вредоносного кода и не совершать на нем финансовых операций до устранения вышеуказанных проблем;

13) в случае обнаружения на техническом устройстве вредоносного кода, вам необходимо немедленно приостановить работу со всеми сервисами финансовых организаций, осуществить совместную с финансовыми организациями проверку на предмет устранения последствий действия вредоносного кода и на предмет наличия или отсутствия несанкционированных действий с использованием ваших учетных данных, и при наличии любых подозрений в возможности совершения с вашего устройства незаконных финансовых операций необходимо незамедлительно обратиться в финансовые организации для осуществления ими процедур по блокировке вашего доступа к сервисам финансовых организаций, обновлению используемого программного обеспечения и замене логинов и паролей доступа к сервисам финансовых организаций.