Рекомендации
по защите информации в целях противодействия незаконным финансовым операциям

Настоящим Акционерное общество Управляющая компания «НРК-Капитал (Эссет Менеджмент)» (далее – Общество) в соответствии с Положением 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» доводит до сведения своих клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям, в том числе информируем:

– о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

– о 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 действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

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.

Под защищаемой информацией понимается:

– информация, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Общества и (или) клиентами Общества (далее - электронные сообщения);

– информация, необходимая Обществу для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться ценными бумагами или иным имуществом;

– информация об осуществленных Обществом и его клиентами финансовых операциях;

– ключевая информация средств криптографической защиты информации, используемая Обществом и его клиентами при осуществлении финансовых операций.

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

Клиенты несут риск финансовых потерь вследствие несанкционированного доступа третьих лиц к защищаемой информации с целью осуществления такими лицами финансовых операций при отсутствии права на их осуществление.

Риск может быть реализован, в том числе, в результате следующих событий:

- утраты (потери, хищения) идентификаторов доступа клиента к системе электронного взаимодействия с Обществом, системам через которые клиент осуществляет финансовые операции, паролей, ключей электронной подписи;
- получение третьими лицами доступа к устройству клиента в результате его утраты (потери, хищения) и получение с помощью него защищаемой информации и (или) доступа к системам, через которые клиент взаимодействует с Обществом, и (или) совершает финансовые операции;
- воздействия вредоносного кода на устройства клиента, в которых содержится защищаемая информация, и (или) с помощью которого клиента осуществляет взаимодействие с

Обществом, и (или) совершает финансовые операции, с целью кражи информации и (или) получения контроля над устройством;

- совершение в отношении клиента иных противоправных действий, направленных на получение защищаемой информации и (или) доступа к устройствам клиента.

2. Важные замечания

Все риски, связанные с утратой и компрометацией учётных данных (логина, пароля) для доступа к системе электронного взаимодействия с Обществом, ключей электронной подписи несет клиент.

Если клиент сомневается в конфиденциальности своих учетных данных и (или) есть подозрение в их компрометации (копировании), клиент должен осуществить действия в целях замены учетных данных, обратившись к оператору СЭД.

Если есть подозрение в компрометации (копировании) ключей электронной подписи или в случае их утраты, клиент должен осуществить действия в целях блокирования ключей электронной подписи, обратившись в организацию, в которой они были получены.

3. Меры по предотвращению несанкционированного доступа к защищаемой информации

3.1. Обеспечьте защиту устройства, с которого вы осуществляете взаимодействие с Обществом. К таким мерам включая, но не ограничиваясь могут быть отнесены:

- использование только лицензированного программного обеспечения, полученного из доверенных источников;
- запрет на установку программ из непроверенных источников;
- наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя;
- настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;
- хранение, использование устройства с целью избежать рисков его утраты (потери, хищения);
- своевременные обновления операционной системы;
- активация парольной или иной защиты для доступа к устройству;
- в случае обнаружения злонамеренного программного обеспечения на устройстве после его удаления незамедлительная смена логина и пароля;
- запрет на осуществление действий, направленных на передачу своей личной информации через общедоступные беспроводные сети. Работая в них, запрет на введение паролей доступа, логинов.

3.2. Обеспечьте конфиденциальность персональных данных и защищаемой информации, в том числе:

- храните в тайне аутентификационные / идентификационные данные и ключевую информацию, полученные от оператора системы электронного взаимодействия с Обществом: пароли, закрытые ключи, сертификаты, а в случае компрометации немедленно примите меры для смены и (или) блокировки;
- соблюдайте принцип разумного раскрытия ваших персональных данных и защищаемой информации, в том числе о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV[1] кодах.

3.3. Проявляйте осторожность и предусмотрительность, в том числе:

- 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 письмо. Входящее письмо может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц;

[1] Card Verification Value/Code, трехзначный защитный код, который находится на обратной стороне банковской карты рядом с полем для подписи

- будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта;
- будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код;
- не заходите в системы удаленного доступа с не доверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- анализируйте информацию в прессе и иных общедоступных специализированных источниках о последних известных критичных уязвимостях и вредоносных кодах;
- осуществляйте звонок в Общество только по номеру телефона, указанному на официальном сайте Общества. Важно учесть, что от лица Общества не могут поступать звонки или сообщения, в которых от вас требуют передать пароль, кодовое слово и т.д.;
- 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 системам, с помощью которых вы осуществляете взаимодействие с Обществом и которыми пользовались вы;
- при утере, краже телефона, планшета, персонального компьютера, иного устройства, используемого для осуществления взаимодействия с Обществом, необходимо:

  a. незамедлительно проинформировать Общество и оператора системы электронного взаимодействия;

  b. по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту;

  c. сменить пароль, воспользовавшись другим доверенным устройством и (или) заблокировать доступ, обратившись к оператору системы электронного взаимодействия;
- при подозрении на несанкционированный доступ и (или) компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и (или) заблокировать доступ к системе, через которую осуществляется взаимодействие с Обществом, обратившись к оператору системы электронного взаимодействия. Если это уместно – отозвать скомпрометированный закрытый ключ в соответствии с правилами, отраженными в договорных и (или) процедурных документах лица, выпустившего такой ключ;
- помните, что наличие резервной копии может облегчить и ускорить восстановление вашего устройства;
- лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у вас;
- контролируйте свой телефон. В случае выхода из строя сим карты, используемой для получения СМС-кодов, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи;
- регулярно выполняйте резервное копирование важной информации;
- поддерживайте вашу контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с вами можно было оперативно связаться.

3.4. При работе с ключами электронной подписи необходимо:

- в случае хранения секретных ключей электронной подписи на внешнем ключевом носителе крайне внимательно относиться к внешнему ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носитель из компьютера, если он не используется для работы;
- использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на устройстве.

3.5. При работе на персональном 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.

3.6. При работе с мобильным устройством необходимо:

- не оставлять свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование;
- использовать только официальные мобильные приложения, загруженные при помощи официального магазина приложений;
- 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.

3.7. При обмене информацией через сеть Интернет необходимо:

- не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте и других приложений, используемых в том числе для обмена сообщениями (электронными письмами), не переходить по содержащимся в таких письмах ссылкам;
- не вводить персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах;
- ограничить посещение сайтов сомнительного содержания;
- не сохранять пароли в памяти интернет-браузера, если к компьютеру (иному устройству) есть доступ третьих лиц;
- не нажимать на баннеры и всплывающие окна, возникающие во время работы с информационно-телекоммуникационной сетью Интернет;
- при скачивании контента надо внимательно читать условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*);
- открывать файлы только известных расширений из доверенных источников.