

УТВЕРЖДЕНО
Решением Единственного Участника
Общества с ограниченной ответственностью
«Управляющая компания «САН»
№7 от 13.07.2021 г.

**Рекомендации по защите информации от воздействия программных кодов,
приводящих к нарушению штатного функционирования средства вычислительной
техники, в целях противодействия незаконным финансовым операциям**

Москва, 2021 г.

1. Общие положения

1.1. Настоящие «Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям» (далее – Рекомендации) разработаны в соответствии с требованиями Положения Банка России №757-П от 20.04.2021 «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» и включают в себя информацию:

- 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.

1.2. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне ООО «Управляющая компания «САН» (далее – Организация), так и на стороне клиента.

1.3. В результате неправомерных действий третьих лиц информация, связанная с проведением финансовых операций, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах Организации, а именно:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Организации и (или) клиентами (далее - электронные сообщения);
- информация, необходимая для авторизации клиента в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- информация об осуществленных финансовых операциях;
- ключевая информация средств криптографической защиты информации (далее - криптографические ключи)

(далее в совокупности – защищаемая информация) может быть подвергнута воздействию вредоносных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее – вредоносный код).

1.4. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах компьютерных вирусов и программ, направленных на разрушение,

нарушение работоспособности или модификацию специализированного и системного программного обеспечения (далее - ПО), либо на перехват информации, в том числе паролей.

- 1.5. 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.
- 1.6. В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Организации, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части не противоречащей положениям внутренних документов.

2. Риски получения несанкционированного доступа к защищаемой информации.

- 2.1. При осуществлении критичных (финансовых) операций следует принимать во внимание риски получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.
- 2.2. Наиболее опасным является кража учетных данных - хищение личных данных клиента Организации и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.
- 2.3. Риски получения третьими лицами несанкционированного доступа к защищаемой информации могут быть обусловлены:
- кражей 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 использованием злоумышленниками указанных данных с других устройств для несанкционированного доступа;
 - установкой на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от Вашего имени;
 - использованием злоумышленником утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Организацией в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту;
 - получением 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 кредитной организации 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;

- перехватом электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Организацией. Или в случае получения доступа к вашей электронной почте, отправка сообщений от вашего имени.

2.4. Риски получения несанкционированного доступа к информации, прежде всего, связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью кражи идентификационных данных), а также воздействием вредоносного кода.

Фишинг – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

2.5. Доступ к информации со стороны третьих лиц может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, об имуществе, переданном в доверительное управление, состоянию счетов, персональных данных, и/или иной информации, имеющей значение для Клиента.

2.6. Нарушение целостности данных (изменение структуры баз данных, связей между таблицами и т.д.), искажение данных или их потеря (удаление информации), в результате злонамеренных действий лица, получивших доступ.

2.7. Компрометация криптографических ключей – факт доступа постороннего лица к информации, содержащей закрытый ключ электронной цифровой подписи, а также подозрение на компрометацию.

2.8. Для минимизации вышеуказанных рисков Организацией предпринимаются все необходимые организационные и технические меры, направленные на предотвращение несанкционированного доступа третьих лиц к информации конфиденциального характера, связанной с использованием информационных систем Организации.

3. Рекомендации по защите информации от вредоносного кода.

3.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

3.2. 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.

- 3.3. Будьте осторожны при просмотре/ работе с интернет сайтами, так как вредоносный код может быть загружен с сайта.
- 3.4. 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 (далее – антивирусное ПО) в автоматическом режиме).
- 3.5. 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.
- 3.6. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.
- 3.7. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).
- 3.8. Не используйте права администратора без необходимости. В повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.
- 3.9. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, старайтесь периодически просматривать журнал событий и реагировать на ошибки.
- 3.10. Обязательно установите и своевременно обновляйте на компьютере лицензионное антивирусное ПО с функцией автоматического обновления вирусных баз. Лечение (удаление) зараженных файлов должно производиться антивирусным ПО в автоматическом режиме.
- 3.11. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода.
- 3.12. Антивирусное ПО должно запускаться автоматически, с загрузкой операционной системы.
- 3.13. Рекомендуется подвергать 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 должно осуществляться в автоматическом режиме.
- 3.14. Исключите возможность бесконтрольного доступа посторонних лиц (гостей, посетителей) к вашим компьютерам. Имейте в виду, что, если вы передаете ваш телефон и/или устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам, которыми пользовались Вы.
- 3.15. Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у вас.
- 3.16. 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.

- 3.17. Не используйте на устройствах программное обеспечение неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств.
- 3.18. Не устанавливайте и не сохраняйте подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты.
- 3.19. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), следует полностью воздержаться от использования систем ЭДО до устранения проблемы.
- 3.20. Помните, что ни Организация, ни оператор ЭДО не несет ответственности в случае возникновения финансовых потерь, понесенных клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука) для доступа к системе ЭДО.

4. Меры по предотвращению несанкционированного доступа к защищаемой информации путем использования ложных (фальсифицированных) ресурсов сети Интернет

- 4.1. Мошеннический или поддельный web-сайт - это небезопасный вебсайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете. Они предназначены для сбора конфиденциальной информации обманным путем.
- Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению идентификационных данных.
- 4.2. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс системы ЭДО, необходимо удостовериться, чтобы при подключении к СЭДО защищённое SSL-соединение было установлено исключительно с официальным сайтом ЭДО.
- 4.3. Перед просмотром электронного письма всегда внимательно проверяйте адрес отправителя. Входящее электронное письмо может быть от злоумышленника, который маскируется под Организацию или иных доверенных лиц. Строка «Отправитель» может содержать адрес электронной почты, который является почти точной копией адреса настоящей компании. Подделать адрес электронной почты отправителя очень просто, поэтому будьте внимательны.
- 4.4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия. Не открывайте вложений, прикрепленных к подобным письмам.
- 4.5. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с <http://> вместо <https://>), не переходите по этой ссылке.

5. Меры по предотвращению получения несанкционированного доступа третьими лицами

- 5.1. Выбирайте пароли самостоятельно. Проводите регулярную смену паролей. Используйте сложные пароли, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками. Не сохраняйте пароли в текстовых файлах на устройстве либо иных электронных носителях.
- 5.2. Рекомендуется выделить отдельный компьютер, который использовать только для работы в системе ЭДО с установленным на нем минимальным необходимым для работы набором программного обеспечения.
- 5.3. Не используйте на устройстве, предназначенном для доступа к системе ЭДО, средства удаленного администрирования.
- 5.4. Используемые в ЭДО логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования.
- 5.5. Использование Ключевого носителя должно осуществляться исключительно владельцем ключа ЭП. Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе) и хранить его в сейфе или запираемом шкафу исключив возможность несанкционированного доступа.
- 5.6. Необходимо отключать и извлекать из компьютера Ключевой носитель, если он не используется для работы в ЭДО. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭП третьими лицами;
- 5.7. Рекомендуется использовать разные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные.
- 5.8. В том случае, если Вы обнаружили, что Ваш пароль от системы ЭДО скомпрометирован или в процессе работы Вы столкнулись с тем, что ранее действовавший пароль не срабатывает и не позволяет Вам войти в систему, рекомендуем незамедлительно принять меры по смене пароля и можно быстрее обратиться к оператору ЭДО для получения инструкций по смене пароля.
- 5.9. Не пересылайте конфиденциальную информацию через электронную почту или SMS-сообщения.
- 5.10. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе ЭДО, для посторонних лиц и персонала, не имеющего отношения к работе с ЭДО.
- 5.11. Необходимо принять меры по контролю за конфигурацией компьютера, с использованием которого осуществляется информационный обмен по ЭДО, и не допускать несанкционированных программно-аппаратных изменений конфигурации.
- 5.12. На компьютере для работы с системой ЭДО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками ЭДО, операционной системы,

web-браузеров (Chrome, Firefox, Opera, IE Explorer и т.д.) и иного прикладного программного обеспечения.

- 5.13. Применять на компьютере для работы с ЭДО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты.
- 5.14. На компьютере для работы с системой ЭДО необходимо исключить посещение web-сайтов сомнительного содержания, загрузку и установку нелегального программного обеспечения и т.п. Использование нелегального программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения конфиденциальных данных.
- 5.15. В случае компрометации или подозрении на компрометацию закрытого ключа ЭП (утрате, потере, хищении) Ключевого носителя необходимо незамедлительно обратиться к оператору ЭДО для блокирования скомпрометированных ключей ЭП.
- 5.16. В случае передачи (списания) компьютера, на котором ранее была установлена система ЭДО, необходимо гарантированно удалить с него все следы работы с системой ЭДО.
- 5.17. Необходимо корректно завершать работу в ЭДО, используя для этого пункт меню «Выйти из системы».
- 5.18. При увольнении ответственного сотрудника, имевшего доступ к Ключевому носителю, уведомить оператора ЭДО об увольнении и действовать в соответствии с положениями Договора на использование системы ЭДО.