Утверждено

Приказом
Генерального директора
Небанковской кредитной организации –
центрального контрагента
«Клиринговый центр МФБ»
(акционерное общество)
№1186 от 15.12.2021 г.

Рекомендации участникам клиринга НКО-ЦК «Клиринговый центр МФБ» (АО) о мерах по предотвращению несанкционированного доступа к защищаемой информации в целях противодействия незаконным финансовым операциям

Небанковская кредитная организация – центральный контрагент «Клиринговый центр МФБ» (акционерное общество) (далее – НКО-ЦК «Клиринговый центр МФБ» (АО)) в целях исполнения требований 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» рекомендует участникам клиринга соблюдение мер обеспечения информационной безопасности для снижения следующих рисков несанкционированного доступа к защищаемой информации:

1. Риски разглашения третьими лицами информации конфиденциального характера: сведений об операциях, подключенных услугах, персональных данных и иной значимой информации.

2. Риски совершения третьими лицами юридически значимых действий, включая: подачу заявок по исполнению обязательств, возникших из договоров, заключённых на организованных и не на организованных торгах, в которых НКО-ЦК «Клиринговый центр МФБ» (АО) не является одной из сторон, а также обеспечение исполнения таких обязательств, подключение и отключение услуг, внесение изменений в регистрационные данные участника клиринга, совершение иных действий против их воли.

3. Риски деструктивного воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию исполнения своих обязательств по договору или невозможности использования сервисов НКО-ЦК «Клиринговый центр МФБ» (АО) и для реализации своих намерений.

В рамках осуществления мер защиты информации от воздействия вредоносного кода, приводящего к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям, а также для предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) участником клиринга устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого участником клиринга совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода, НКО-ЦК «Клиринговый центр МФБ» (АО) рекомендует:

- организовать режим эксплуатации устройства, с использованием которого совершаются действия в целях осуществления финансовой операции (далее – устройство) таким образом, чтобы исключить возможность его несанкционированного использования;

- не устанавливать программное обеспечение, полученное из сомнительных источников (например, скаченное с файлообменников и торрентов);
- своевременно устанавливать обновления операционной системы и интернет-браузера вашего устройства, выпускаемые компанией-производителем для устранения выявленных в них уязвимостей;
- своевременно устанавливать последние обновления информационных систем НКО-ЦК «Клиринговый центр МФБ» (АО) всегда использовать средства межсетевого экранирования (брандмауэр или firewall);
- ограничить права пользователя, использующего устройство, минимально необходимыми для работы с системой. Пользователь не должен обладать административными привилегиями;
- в случае утери компьютера/мобильного (переносного) устройства, с которого осуществляются финансовые операции, необходимо выполнить действия, предусмотренные в случае компрометации или утери логина или пароля.

Рекомендации по защитным мерам для автоматизированного рабочего места клиента (АРМ):

- средствами BIOS на АРМ следует исключить возможность загрузки операционной системы, отличной от установленной на жёстком диске, т.е. должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB-flash дисков, загрузка по сети и т.п.;
- доступ к изменению настроек BIOS АРМ, должен быть защищён паролем;
- на АРМ необходимо использовать только лицензионное системное и прикладное программное обеспечение;
- на АРМ должна быть установлена только одна операционная система;
- на АРМ рекомендуется своевременно проводить обновления системного и прикладного программного обеспечения;
- на АРМ должны быть установлены и регулярно обновляться антивирусные программы (например, Kaspersky, Dr.Web). Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов и другого вредоносного программного обеспечения;
- локальными (или доменными) политиками на АРМ рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему;
- не устанавливать и не использовать на АРМ программы для удалённого управления (например: TeamViewer, Radmin, Ammyy Admin др.);
- для доступа к информационным системам не используйте общедоступные компьютеры (например, установленные вне контролируемой зоны), публичные беспроводные сети (бесплатный Wi-Fi и прочее).
- по возможности, для доступа к автоматизированным системам осуществления финансовых операций используйте выделенный АРМ.

Рекомендации по парольной защите:

- не записывайте пароли, служащие для доступа к устройству на бумажных носителях или в файлах на жестком диске вашего компьютера. Не сообщайте их другим лицам, в том числе вашим родственникам или системным администраторам вашей компании;
- следует использовать специализированное программное обеспечение – менеджеры паролей, для генерации и хранения сложных паролей;
- рекомендуется использовать для доступа к устройству сложные пароли, удовлетворяющие следующим требованиям:
    - длина пароля: минимальная - 8 символов, рекомендуемая – не менее 12 символов;
    - в числе разрешенных символов пароля обязательно должны присутствовать три группы символов из следующих четырёх: прописные буквы строчные буквы, цифры, специальные символы (!"#$%&()``*+,-/:;<=>?);
    - пароль не должен включать в себя легко вычисляемые сочетания символов, не должен содержать имени пользователя, дату рождения, номер телефона, а также названия автоматизированных систем или общепринятые сокращения (Pbvf2022!, zima2022);
    - периодичность смены пароля в информационных системах осуществления финансовых операций должна составлять не более 90 дней;

- не используйте один и тот же пароль для разных систем, в том числе не используйте пароль от информационных систем осуществления финансовых операций для доступа к ресурсам сети Интернет (социальные сети, веб-сайты, доски объявлений);
- в качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке (1qaz@WSX, 1q2w3e4r5t, Qwer!234);
- при смене пароля новый пароль не должен совпадать с ранее используемыми паролями.

Рекомендации по антивирусной защите:

- на АРМ должно быть установлено и регулярно обновляться средство защиты от воздействия вредоносного кода. Рекомендуется установить по умолчанию максимальный уровень политики безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов и другого вредоносного программного обеспечения;
- средство защиты от воздействия вредоносного кода должно быть настроено на работу в автоматическом режиме;
- не реже одного раза в неделю проводите полное антивирусное сканирование устройства. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы;
- установите пароль на отключение средства защиты от воздействия вредоносного кода;
- не отключайте средство защиты от воздействия вредоносного кода, ни при каких обстоятельствах.

Рекомендации по защите АРМ при использовании сети Интернет:

- настройте безопасный режим в обозревателе сети Интернет;
- не посещайте сайты сомнительного содержания;
- не соглашайтесь на установку дополнительного программного обеспечения;
- добавьте в раздел избранное обозревателя сети Интернет наиболее часто посещаемые ресурсы сети Интернет;
- не открывайте вложения электронных писем, полученные от неизвестных вам адресатов. Подобные письма лучше немедленно удалить;
- проверяйте наименование адресата, от которого вам пришло электронное письмо;
- настройте СПАМ-фильтры клиентов электронной почты.

Рекомендации по эксплуатации на АРМ внешнего ключевого носителя:

- для повышения уровня безопасности хранения ключей электронной подписи (далее - ЭП) используйте устройства строгой аутентификации и хранения данных, что позволит существенно снизить вероятность хищения ключей ЭП злоумышленниками;
- для надёжной защиты ключа ЭП рекомендуется установить надёжные пароли;
- внешний ключевой носитель должен храниться только у тех лиц, которым он принадлежит;
- во время работы с внешним ключевым носителем доступ к ним посторонних лиц должен быть исключён;
- для хранения внешнего ключевого носителя должны применяться металлические шкафы и сейфы;
- уничтожение ключей ЭП может производиться путём физического уничтожения внешнего ключевого носителя, на котором они расположены, или путём стирания без повреждения внешнего ключевого носителя (для обеспечения возможности его многократного использования);
- в случае компрометации или подозрения на компрометацию ключа ЭП владелец сертификата ключа ЭП прекращает обмен электронными документами с использованием скомпрометированного ключа и незамедлительно информирует Удостоверяющий центр, выдавший сертификат ключа ЭП, о компрометации посредством любого вида связи с целью блокировки ключа ЭП.

Предотвращение несанкционированного доступа к защищаемой информации:

- не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона и другие данные;
- не открывайте подозрительные файлы, поступившие вам по электронной почте;
- не отвечайте на полученное подозрительное сообщение и не переходите по ссылкам, указанным в сообщении;
- проверяйте параметры операций в сообщениях;
- в случае принуждения вас к установке дополнительного программного обеспечения – прервите контакт;
- в случае возникновения подозрений на мошенничество как можно скорее сообщите в НКО-ЦК «Клиринговый центр МФБ» (АО) о происшествии.