Приложение №1
к приказу № 116/1 от «21» февраля 2020 г.

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

Акционерное общество «Клиринговый центр МФБ» (далее – КЦ МФБ) в целях исполнения требований Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, а также для противодействия осуществлению незаконных финансовых операций», рекомендует участникам клиринга соблюдение мер обеспечения информационной безопасности в целях снижения следующих рисков несанкционированного доступа к защищаемой информации:

1. Доступ со стороны третьих лиц может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, подключенных услугах, персональных данных и иной значимой информации.

2. Доступ со стороны третьих лиц может повлечь за собой совершение юридически значимых действий, включая: подачу заявок по исполнению обязательств, возникших из договоров, заключённых на организованных и не на организованных торгах, в которых КЦ МФБ 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. Доступ со стороны третьих лиц может повлечь за собой деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию исполнения своих обязательств по договору или невозможности использования сервисов КЦ МФБ и для реализации своих намерений.

В рамках защиты информации от воздействия программных кодов, приводящих 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, КЦ МФБ 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 КЦ МФБ 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).

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;
- рекомендуется использовать для доступа к устройству сложные пароли, удовлетворяющие следующим требованиям:
- длина пароля должна быть не менее 8 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;
- периодичность смены пароля должна составлять не менее 30 дней;
- в качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;
- при смене пароля новый пароль не должен совпадать с ранее используемыми паролями; не использовать последние 24 пароля.

Рекомендации по антивирусной защите:

- для защиты от вредоносного программного обеспечения необходимо использовать лицензионное антивирусное программное обеспечение, функционирующее в автоматическом режиме;
- антивирусное программное обеспечение должно регулярно обновляться;
- не реже одного раза в неделю проводите полное антивирусное сканирование устройства. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы;
- не отключайте антивирусное программное обеспечение, ни при каких обстоятельствах.

Рекомендации по защите АРМ при использовании сети Интернет:

- не посещайте сайты сомнительного содержания;
- не открывайте вложения электронных писем, полученные от неизвестных вам адресатов. Подобные письма лучше немедленно удалить.

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 позволяет 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 Клиент, Владелец Квалифицированного сертификата, прекращает обмен электронными документами с использованием скомпрометированного ключа и незамедлительно информирует Удостоверяющий центр о компрометации посредством любого вида связи с целью блокировки ключа ЭП.

Предотвращение несанкционированного доступа к обрабатываемой информации:

К компрометации ключей можно отнести следующие события:

- утрата ключевого носителя (в том числе с последующим обнаружением); хищение;
- несанкционированное копирование; передача ключевой информации по каналам связи в открытом виде;

- увольнение сотрудников, имевших доступ к ключевой информации; любые другие виды разглашения ключевой информации, в результате которых ключи могут стать доступны лицам, к ним не допущенным;
- не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли 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.