Приложение 1
к приказу №01/01-62 от «28» мая 2019 г.

РЕКОМЕНДАЦИИ
клиентам ООО «АФМ» по защите информации в целях противодействия незаконным финансовым операциям

Деятельность, связанная с использованием на рынке доверительного управления активами электронно-вычислительной техники, коммуникационных устройств, несет в себе риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления от имени клиента ООО «АФМ» или его уполномоченного лица финансовых операций, которые могут нанести ущерб интересам клиента ООО «АФМ».

К защищаемой относится следующая информация:

– информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками ООО «АФМ» и (или) клиентами ООО «АФМ» либо их уполномоченными лицами;

– информация, необходимая ООО «АФМ» для авторизации клиентов и их уполномоченных лиц при осуществлении финансовых операций и удостоверении прав распоряжаться денежными средствами, ценными бумагами или иным имуществом;

– информации об осуществленных ООО «АФМ» и его клиентами финансовых операциях;

– ключевая информация средств криптографической защиты информации, используемая ООО «АФМ» и его клиентами при осуществлении финансовых операций.

Реализация риска получения третьими лицами, в том числе злоумышленниками, несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций может произойти, в частности, в результате доступа третьих лиц к контролю конфигурации устройств, с использованием которых клиентами ООО «АФМ» совершаются действия в целях осуществления финансовых операций, получение доступа третьих лиц к идентификационным данным клиентов ООО «АФМ», с использованием которых осуществляется авторизация совершения клиентами финансовых операций.

Доступ третьих лиц к контролю конфигурации устройств, с использованием которых клиентами ООО «АФМ» совершаются действия в целях осуществления финансовых операций, может быть осуществлен в результате утраты (потери, хищения) такого устройства, утраты клиентом контроля за ним, а также в результате воздействия на него вредоносного программного кода.

В целях минимизации риска получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций ООО «АФМ» рекомендует своим клиентам и их уполномоченным лицам применять, в том числе, но не ограничиваясь, следующие меры.

1. Обеспечение безопасности компьютера, средств электронно-вычислительной техники, коммуникационных устройств, с использованием которых осуществляются финансовые операции:

– использование только лицензионного программного обеспечения, полученного из легального источника;

– регулярное обновление операционных систем и установленного программного обеспечения устройства, получение обновлений операционных систем и установленного программного обеспечения только из легального источника;

– использование антивирусного программного обеспечения и его регулярное обновление, получение антивирусного программного обеспечения и его обновлений только из легального источника;

– ограничение доступа к устройствам посторонних лиц;

– использование функций автоматической блокировки устройств в случае неиспользования и утери (в том числе – кратковременной) контроля устройств;

– обеспечение контроля действий третьих лиц при обслуживании и ремонте устройств.

2. Соблюдение правил безопасного использования информационно-телекоммуникационной сети Интернет:

– ограничение использования сомнительных интернет - ресурсов, сайтов социальных сетей, программ и сервисов обмена мгновенными сообщениями;

– не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скачанные с неизвестных интернет - сайтов, присланные по электронной почте с неизвестных адресов от неизвестных отправителей;

– не отвечать на подозрительные сообщения, полученные с неизвестных адресов.

3. Обеспечение безопасности авторизационных и идентификационных данных, учетных записей, паролей доступа:

– использование надежных паролей, содержащих не менее 8 различных символов (сочетание букв/цифр, большого/малого регистра);

– не допускается использование в паролях и условных фразах общеизвестных или широко известных сведений о клиентах (имена, фамилии, даты рождения, адреса проживания, марки и номерные знаки автомобилей клиентов и их родственников и т.п.);

– не допускается открытая передача паролей, авторизационных и идентификационных данных клиентов, их хранение в открытом виде, в браузерах, на бумажных носителях;

– регулярное обновление паролей;

– не допускается использование типовых паролей для доступа к различным системам, используемым клиентами.

4. Обеспечение безопасности ключей электронной подписи (ключей ЭП) и использования средств криптографической защиты информации:

– хранение в тайне ключей ЭП и обеспечение сохранности ключей ЭП и ключевого носителя;

– применение всех возможных мер для предотвращения потери ключей ЭП, раскрытия, искажения и несанкционированного использования ключей ЭП;

– применение только сертифицированного программного обеспечения средств криптографической защиты информации, полученного из легального источника;

– немедленное обращение в организацию (удостоверяющий центр), выпустившую ключи ЭП, с заявлением на прекращение действия сертификата в случае потери, раскрытия, искажения ключа ЭП, в случае, если стало известно, что этот ключ ЭП используется или использовался ранее другими лицами, а также в иных случаях компрометации ключа ЭП или при подозрениях на его компрометацию.

5. Обеспечение безопасности при использовании сервисов удаленного выполнения финансовых операций:

– для подключения и работы с сервисами не допускается использование компьютера, средств электронно-вычислительной техники, коммуникационных устройств третьих лиц;

– не допускается подключение и работа с сервисами с устройств, использующих подключение к общедоступной Wi-Fi сети;

– обязательное использование при подключении и работе с сервисами безопасного сетевого соединения с сервисами по протоколу HTTPS;

– немедленное прекращение работы с сервисами в случае подозрения на заражение устройств вредоносным программным кодом с уведомлением уполномоченных сотрудников ООО «АФМ».

При невыполнении или неполном выполнении настоящих рекомендаций Вы принимаете на себя риск осуществления финансовых операций от Вашего имени лицами, не обладающими правом распоряжения Вашими финансовыми средствами.

Настоящие рекомендации о рисках получения несанкционированного доступа к защищаемой информации, о защите информации от воздействия вредоносных кодов и их своевременному выявлению и нейтрализации, о мерах по предотвращению несанкционированного доступа к защищаемой информации, доводятся ООО «АФМ» до сведения клиентов на основании требований Положения 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 № 684-П, утвержденного Банком России 17.04.2019 г.