РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

В соответствии с требованиями Положения Банка России от 20.04.2021 № 757-П[1] Акционерное общество АО ВТБ Специализированный депозитарий доводит до вашего сведения основные рекомендации по соблюдению информационной безопасности:

1. В отношении защиты информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

Для защиты информации от воздействия вредоносного кода необходимо:

- на средствах обработки и передачи информации (автоматизированное рабочее место пользователя, почтовый сервер, системы хранения данных, информационные системы и т.д) использовать лицензионное антивирусное программное обеспечение (далее - АВЗ), функционирующее в автоматическом режиме;
- базы данных АВЗ должны своевременно обновляться (предпочтительно в автоматическом режиме);
- не реже одного раза в неделю проводите полное антивирусное сканирование средств обработки и передачи информации. Настройка АВЗ должна обеспечить в случае обнаружения подозрительные объекты должны быть удалены, а при невозможности удаления – заблокированы;
- запретить отключение АВЗ;
- использование только лицензированного программного обеспечения, полученного из доверенных источников;
- своевременное обновление операционной системы устройства и используемого в работе прикладного программного обеспечения;
- не посещайте сайты сомнительного содержания, использовать фильтрацию доступа к WEB – ресурсам;
- не используйте для работы компьютеры, расположенные в местах общего пользования (отелях, бизнес-центрах), а также общедоступные каналы связи (открытые сети Wi-Fi);
- при работе с электронной почтой всегда проверяйте адрес отправителя, не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

2. Информация о возможных рисках несанкционированного доступа (далее - НСД) к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Риски НСД могут возникать вследствие:

---

[1] «Положение 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», (утв. Банком России 20.04.2021 N 757-П)

- утраты пользователем пароля и/или идентификатора доступа к информационным системам, иных конфиденциальных данных, таких как - закрытый ключ/токен, посредством технических средств и/или вредоносного кода и использовании злоумышленниками указанных данных с других устройств для несанкционированного доступа;

− внедрение на устройство вредоносного кода, который позволит злоумышленникам осуществить несанкционированный доступ к информационным ресурсам и провести финансовые операции от имени клиента Компании;

− использования злоумышленником утерянного или украденного мобильного устройства для получения СМС кодов, которые могут применяться Компанией в качестве способа идентификации Клиента;

− кражи или несанкционированного доступа к устройству, с использованием которого клиент Компании пользуется услугами Компании для получения данных и/или несанкционированного доступа к услугам с этого устройства;

− получения злоумышленниками персональных данных клиента Компании, пароля и идентификатора доступа и/или кода из СМС и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием.

3. Информации 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, информация в отношении контроля конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода:

− выполнения всех рекомендаций, перечисленных в п.1;

− настройка прав доступа к обработке и передачи информации таким образом, чтобы несанкционированный доступ к информации на таком устройстве был невозможен даже при утрате устройства владельцем (физическая защита, MDM, многофакторная аутентификация и т.д.);

− использование устройства способом, исключающим или значительным образом снижающем возможность его кражи или утери;

− для доступа к устройству использовать надежные пароли (сочетание букв/цифр, большого/малого регистра) и многофакторную аутентификацию. Регулярное обновление паролей;

− передача защищаемой информации только через доверенные сети;

− использовать при повседневной работе пользовательские права, не позволяющие вносить изменения в конфигурацию устройства;

− осуществлять периодический контроль журналов АВЗ, системных журналов, перечней установленных программ, запущенных процессов и подключаемых устройств.

4. Обеспечение безопасности при работе с ключами электронной подписи:

− для хранения ключей электронной подписи использовать внешние носители;

− обеспечить сохранность носителей ключа электронной подписи, не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы;

− использовать надежные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на устройстве;

− рекомендуется подписание значимых финансовых документов двумя ЭП ответственных лиц;

− рекомендуется сравнение подписанных ЭП финансовых документов с информацией из базы данных, на основе которой был сформирован финансовый документ.