УТВЕРЖДЕНО
Приказом Генерального директора
АО «Биржа «Санкт-Петербург»
от «13» 11 2019 г. № 124

Акционерное общество «Биржа «Санкт-Петербург» (далее – Биржа) в целях соблюдения 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, утвержденного Центральным банком Российской Федерации (Банком России) 17.04.2019 № 684-П настоящим уведомляет участников торгов о возможных рисках получения 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, иной значимой информации.

2. Доступ со стороны третьих лиц может повлечь за собой совершение юридически значимых действий, включая: подачу заявок для заключения договоров на Бирже, заключение договоров, предоставление на Биржу информации о заключенных не на организованных торгах договорах, подключение и отключение услуг, внесение изменений в регистрационные данные участника торгов, совершения иных действий против воли участника торгов.

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 своевременного исполнения своих обязательств по договору или невозможности использования сервисов Биржи для реализации своих намерений.

В рамках защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства 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 устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого участником совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода, Биржа рекомендует следующее:

1. Рекомендуется организовать режим использования устройства, с использованием которого совершаются действия в целях осуществления финансовой операции (далее – «устройство») таким образом, чтобы исключить возможность его несанкционированного использования.

2. Используйте на вашем устройстве только лицензионное программное обеспечение, не устанавливайте программное обеспечение, полученное из сомнительных источников (например, скачанное с файлообменников или торрентов).

3. Устанавливайте обновления операционной системы и интернет-браузера вашего устройства, выпускаемые компанией-производителем для устранения выявленных в них уязвимостей.

4. Устанавливайте последние обновления торговой системы Биржи.

5. Всегда используете встроенные средства межсетевого экранирования (брандмауэр или firewall) операционной системы.

6. Рекомендуется ограничить права пользователя, использующего устройство, минимально необходимыми для работы с системой. Пользователь не должен обладать административными привилегиями.

7. В случае утери компьютера, с которого осуществляются финансовые операции, необходимо выполнить действия, предусмотренные в случае компрометации или утери логина или пароля.

Рекомендации по использованию парольной защиты:

1. 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.

2. Рекомендуется использовать для доступа к устройству сложные пароли, удовлетворяющие следующим требованиям:

- длина пароля должна быть не менее 8 символов;
- пароль должен состоять как минимум из символов трех приведенных далее групп: букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр (0-9), специальных символов и знаков пунктуации (например !@#$%^&*(),.?)

3. Не используйте простые пароли, представляющие собой осмысленные слова (password), дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов (qwerty), последовательности трех и более повторяющихся символов (77777777, 111adZZZ).

Антивирусная защита:

1. Для защиты от вредоносного программного обеспечения необходимо использовать лицензионное антивирусное программное обеспечение, функционирующее в автоматическом режиме.

2. Антивирусное программное обеспечение должно регулярно обновляться.

3. Не реже одного раза в неделю проводите полное антивирусное сканирование устройства. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы.

4. Не отключайте антивирусное программное обеспечение ни при каких обстоятельствах.

Рекомендации по защите при использовании сети Интернет:

1. Не посещайте сайты сомнительного содержания.

2. Не открывайте вложения электронных писем, полученные от неизвестных вам адресатов. Такие письма лучше немедленно удалить.