

Рекомендации по информационной безопасности

Несанкционированный доступ к устройствам (т.е. любому техническому средству, включая, но, не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон, с помощью которого клиент осуществляет вход в автоматизированные системы для совершения финансовых операций или получения информации в отношении таких операций (далее - Системы)), влечет риск получения третьими лицами логина и пароля, используемых для входа в Системы, что может повлечь за собой получение несанкционированного доступа к защищаемой информации.

Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, о состоянии инвестиционного портфеля, другой значимой информации.

Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими третьими лицами юридически значимых действий, включая, но, не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента, и иных действий, совершенных без воли клиента, и направленных против его интересов.

Для минимизации вышеуказанных рисков Обществом предпринимаются меры организационного и технического характера, направленные на предотвращение доступа третьих лиц к защищаемой информации, в то же время, для снижения вышеуказанных рисков, а также для обеспечения необходимого и достаточного уровня информационной защиты, Общество доводит до сведения своих клиентов рекомендации по соблюдению информационной безопасности и рекомендует следующее:

Обеспечение безопасности устройства:

- Блокировать устройства после использования. Использовать настройки устройства, требующие ввода пароля для его разблокировки и использования.
- Не передавать третьим лицам и не оставлять устройства без присмотра.

Использование программного обеспечения на устройстве:

- Использовать на устройствах антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО и входящих в его состав баз вирусных определений в актуальном состоянии.
- Регулярно проводить полную проверку устройства на вирусы и вредоносный код.

- Прекратить использование устройства в случае обнаружения вирусов и вредоносного кода, до момента полного удаления вирусов и вредоносного кода.
- Использовать на устройствах исключительно лицензионное ПО и операционные системы.
- Регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на устройствах.
- Не использовать на устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств.
- Исключить использование средств удаленного администрирования на устройствах.

Безопасность паролей:

- Выбирать пароли самостоятельно. Проводить регулярную смену паролей.
- Использовать сложные пароли, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками.
- Не сохранять пароли в текстовых файлах на устройстве либо иных электронных носителях.
- Не хранить пароль совместно с устройством.
- Не передавать третьим лицам пароли, коды доступа к устройству, а также пароли доступа в Системы.

Соблюдение правил безопасности в сети Интернет:

- При использовании Систем удостовериться в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с https, либо используется значок в виде замка).
- При наличии на устройстве программ фильтрации сетевого трафика (брандмауэра) держать его включённым и блокировать все незнакомые или подозрительные подключения.
- Не отвечать на подозрительные сообщения, полученные с неизвестных адресов.
- Не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скачанные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты.
- Не открывать и не использовать сомнительные Интернет - ресурсы на устройстве.

Осуществление контроля подключения:

- Не использовать устройства третьих лиц для подключения к Системам для совершения финансовых операций или получения информации в отношении таких операций.
- Не работать в Системах с устройства, использующего подключение к общедоступной wi-fi сети.

Незамедлительно информировать Общество в случаях:

- Совершения или подозрения на совершение третьими лицами мошеннических действий с использованием Систем.
- Компрометации или подозрения на компрометацию персонального пароля, логина, мобильного телефона.

Дополнительные рекомендации:

- Соблюдать конфиденциальность и осуществлять защиту от несанкционированного доступа имени пользователя, адреса электронной почты, логина и пароля, а также кодов, полученных при использовании Систем через СМС-сообщения, отправляемых на номер мобильного телефона.
- В случае утери мобильного телефона, незамедлительно обратиться к оператору сотовой связи для осуществления блокировки сим-карты.
- Для связи с Обществом по телефону необходимо использовать только номер телефона, указанный на официальном сайте Общества в сети Интернет.

Как защитить свой аккаунт на «Госуслугах»

Включите двухэтапную проверку входа

После включения двухфакторной аутентификации, чтобы войти в учетную запись, будет необходимо ввести одноразовый СМС-код, который придет на телефон, указанный в госуслугах.

Чтобы включить двухэтапную проверку:

- Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет
- На главной странице личного кабинета откройте вкладку Настройки
- Нажмите Настройка безопасности
- Выберите Включить двухэтапную проверку входа
- Введите пароль от аккаунта и нажмите Включить

Используйте уникальный пароль

Уникальный и сложный пароль позволит защитить ваш аккаунт от классического перебора паролей. Однако не стоит использовать один и тот же пароль на всех ресурсах. Кража данного пароля на одном из сервисов позволит злоумышленникам получить доступ ко всем вашим ресурсам, где использовался данный пароль. Поэтому при задании нового пароля используйте генераторы паролей.

Включите оповещения о входе в ваш аккаунт Госуслуг

Включение уведомлений позволит вам контролировать доступ к вашему аккаунту. Уведомления позволят отследить несанкционированный доступ и позволят оперативно принять меры, в частности произвести смену пароля.

Чтобы включить уведомления:

- Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет.
- На главной странице личного кабинета откройте вкладку Настройки.
- Нажмите Настройки безопасности.
- В блоке Оповещения о входе поставьте флажок Присылать уведомление на электронную почту.

Задайте контрольный вопрос

Контрольный вопрос является дополнительной мерой для защиты аккаунта. Необходимо, чтобы ответ на контрольный вопрос знали только вы, и его нельзя было бы найти с помощью поисковых систем в интернете.

Чтобы задать контрольный вопрос:

- Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет.
- На главной странице личного кабинета откройте вкладку Настройки.
- Нажмите Настройки безопасности.
- Выберите Задать контрольный вопрос.
- Введите вопрос, ответ на него и пароль.
- Нажмите .

Включите вход с помощью электронной подписи:

При наличии квалифицированной электронной подписи, вы можете использовать ее, для авторизации.

Чтобы включить вход с помощью электронной подписи:

- Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет.
- На главной странице личного кабинета откройте вкладку Настройки.
- Нажмите Настройки безопасности.
- Выберите Включить вход с помощью электронной подписи.
- Введите пароль от аккаунта и нажмите Включить.