Приказом Генерального директора
ООО «Проектная фондовая компания»
№ 25-12-23/1-ОД от 23.12.2025

РЕКОМЕНДАЦИИ КЛИЕНТАМ
по соблюдению мер информационной безопасности
при использовании информационных ресурсов

Рекомендации по защите информации от воздействия вредоносного кода и по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

1. Общие положения

1.1. Задачи защиты информации сводятся к возможности минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне ООО «Проектная фондовая компания» (далее – Компания), так и на стороне клиента.
1.2. Наиболее опасным является кража учетных данных – хищение личных данных клиента и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.
1.3. Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом». «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.
1.4. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.
«Трояны» - специализированные вредоносные программы для похищения личных данных пользователей и их незаконного использования для выполнения несанкционированных операций от имени клиента.
Трояны распространяются по электронной почте, по каналам сервисов мгновенной передачи информации и через принадлежащие злоумышленникам сайты.
1.5. Средства и методы защиты информации, применяемые в Компании, позволяют обеспечить необходимый уровень безопасности при осуществлении брокерских и депозитарных операций и предотвратить мошеннический вывод активов (ценных бумаг, производных финансовых инструментов, денежных средств и т.д.) со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

2. Рекомендации по защите информации от воздействия вредоносного кода

2.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
2.2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.
2.3. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).
2.4. Не используйте права администратора при отсутствии необходимости, а в повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.
2.5. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.
2.6. Не используйте на устройстве, предназначенного для доступа к системе электронного документооборота (далее – ЭДО) или к торговой системе (далее ТС), средства удаленного администрирования.

2.7. Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Удаление зараженных файлов производится антивирусным средством в автоматическом режиме.
2.8. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.
2.9. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.
2.10. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.
2.11. При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.
2.12. При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.
2.13. Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе ЭДО или ТС.
2.14. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ.
2.15. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты.
Старайтесь не использовать компьютер, с которого Вы осуществляете операции с Вашими активами, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.
2.16. Важно знать, что надежным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.
2.17. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования ЭДО и ТС и проведения операций до исправления ситуации.
2.18. **Помните**, что Компания не несет ответственности в случае возникновения финансовых потерь, понесенных Клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука) для доступа к ТС и/или системе ЭДО.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

3.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете, и предназначены для сбора конфиденциальной информации обманным путем.
3.2. Злоумышленниками возможно создание фальсифицированных WEB-сайтов – их доменные имена и стили оформления могут имитировать сайт Компании и содержать ложные банковские реквизиты и контактную информацию. Вступление в какие- либо деловые отношения с лицами, представляющими ложную Компанию и использование подобных реквизитов, рискованно и может привести к нежелательным последствиям. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению идентификационных данных. Помните, что сайты, визуально напоминающие сайт Компании или личный кабинет клиента на сайте Компании, создаются специально для незаконного получения информации.

В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта или ЭДО, пожалуйста, незамедлительно сообщите об этом по контактным телефонам Компании 8(800) 500-07-86 или на адрес электронной почты: privacy@pfc.ru

3.3. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Компанией в системе ЭДО, и (или) использующих зарегистрированные товарные знаки и наименование Компании, необходимо удостовериться, чтобы при подключении к ЭДО защищённое SSL-соединение было установлено исключительно с официальным сайтом ЭДО. Прежде чем ввести логин и пароль, Клиентам необходимо проверить по информации из SSL-сертификата подлинность сайта.

3.4. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.5. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.6. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Компания всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.7. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашим активам угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.8. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуется выделить отдельный компьютер, который использовать только для работы в системе ЭДО или ТС.

4.2. Рекомендуется регулярно менять пароль для работы со своими учетными данными в ЭДО. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.3. Используемые в ЭДО и ТС логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам.

4.4. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать логин и пароль к ЭДО и ТС там, где доступ к нему могут получить посторонние лица.

4.5. Генерацию рабочих ключей для ТС осуществляется владельцем ключа ЭП самостоятельно.

4.6. Использование Ключевого носителя должно осуществляться исключительно владельцем ключа ЭП. Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе или дискете) и хранить его в сейфе или запираемом шкафу исключив возможность несанкционированного доступа.

4.7. Необходимо отключать, извлекать Ключевой носитель, если он не используются для работы в ЭДО. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭП третьими лицами;

4.8. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем брокерском, депозитарном или банковском счете и т. д.).

4.9. В том случае, если Вы обнаружили, что Ваш пароль от ТС скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 4.1.
4.10. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Компанию для получения инструкций по смене пароля.
4.11. Никому не разглашайте пароль от ТС и ЭДО. Компания не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).
4.12. Не пересылайте файлы с конфиденциальной информацией для работы в ТС или ЭДО по электронной почте или через SMS-сообщения.
4.13. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе, персонала, не имеющего отношения к работе с ТС и/или ЭДО и посторонних лиц.
4.14. Незамедлительно обращайтесь в Компанию в том случае, если Вы получили уведомление об операции или сделке, которую Вы не проводили.
4.15. Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, используемые для доступа в систему, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение;
4.16. Принять меры по контролю конфигурации компьютера, с использованием которого осуществляются операции и сделки через ТС и ЭДО, и её изменения. Не допускать несанкционированных программно-аппаратных изменений конфигурации.
4.17. На компьютере для работы с ТС и ЭДО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками операционной системы, web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Opera и т.д.) и иного прикладного программного обеспечения.
4.18. Применять на компьютере для работы с ТС и ЭДО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты.
4.19. Рекомендуется применять на компьютере для работы с ТС и ЭДО специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.
4.20. На компьютере для работы с ТС и ЭДО необходимо исключить посещение WEB- сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения Ваших активов.
4.21. Не допускается работать с ТС и ЭДО на компьютерах в Интернет-кафе или на других компьютерах общего пользования (вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых рабочих мест увеличивает риск неправомерного использования ключа ЭП и другой аутентификационной информации.
4.22. Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере для работы с ТС и ЭДО и работу с указанными системами на компьютере осуществлять только под учетной записью с ограниченными правами в операционной системе. Не допускать штатную работу в ЭДО под учетной записью с правами администратора в операционной системе компьютера.
4.23. В случае компрометации или подозрении на компрометацию закрытого ключа ЭП, для предотвращения несанкционированного доступа к управлению счетами, в том числе при утрате (потере, хищении) Ключевого носителя, с использованием которого Клиент осуществляет операции и сделки, Клиенту необходимо незамедлительно обратиться в Компанию для блокирования скомпрометированных ключей ЭП.
4.24. Регулярно контролировать состояние своих счетов и незамедлительно сообщать в Компанию обо всех подозрительных или несанкционированных изменениях.
4.25. При обслуживании компьютера сотрудниками технической поддержки организации Клиента или сторонних организаций – обеспечивать контроль выполняемых ими действий.

4.26. Не передавать Ключевой носитель сотрудникам технической поддержки для проверки работы ТС или ЭДО, проверки настроек взаимодействия с Компанией и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить Ключевой носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейсе ТС или ЭДО, и лично ввести пароль, не допуская ознакомления с ним посторонних лиц.
4.27. В случае передачи (списания) компьютера, на котором ранее была установлены ТС или ЭДО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Клиента, в том числе следы работы в этих системах.
4.28. Необходимо корректно завершать работу в ТС и ЭДО, используя для этого пункт меню «Выйти из системы».

5. Рекомендации по безопасности при использовании мобильных устройств для доступа к ТС или ЭДО

5.1. Не совмещайте устройства доступа к ТС и/или ЭДО и устройства получения SMS-сообщений с подтверждающим одноразовым паролем (например, мобильный телефон, смартфон или планшет).
5.2. При утрате мобильного телефона, на который Вы получаете сообщения с SMS-паролем, сразу же обратитесь к оператору сотовой связи и заблокируйте SIM-карту.
5.3. При потере мобильного телефона с подключенными ТС и /или ЭДО следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Компанию для блокировки доступа.
5.4. При смене номера телефона, на который подключена ТС, необходимо отключить услугу от старого номера телефона и подключить услугу на новый номер. Помните, что операторы сотовой связи могут передать номер телефона другому абоненту, если он будет неактивным длительное время.
5.5. Будьте внимательны - не оставляйте свой телефон без присмотра, чтобы исключить несанкционированный доступ к Вашим данным. Установите на телефоне пароль, данная возможность доступна для любых современных моделей телефонов/смартфонов.
5.6. Не подключайте ТС на телефоны, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Компании.
5.7. При установке на телефон дополнительных программ обращайте внимание на полномочия, которые необходимы программе. Если программе требуются излишние полномочия это повод проявить настороженность. Обращайте внимание на такие опасные разрешения: доступ и отправка SMS, доступ к Интернет.
5.8. Установите на телефон антивирусное ПО и своевременно его обновляйте.
5.9. При внезапном прекращении работы SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин - в отношении Вас возможно проведение мошеннических действий третьими лицами.
5.10. Не взламывайте телефон, так как это отключает защитные механизмы, заложенные производителем. В результате ваш телефон становится уязвимым к заражению вирусным ПО.