Об угрозах, рисках и мерах информационной безопасности при проведении электронных торгов

Инструкция для клиентов электронной торговой площадки

ЗАО «Сбербанк-АСТ»

(редакция от 24.07.2014)

1. Введение

Электронные торги – как и другие виды деятельности, связанные с распределением финансовых средств, являются объектом внимания и воздействия киберпреступников.

В целях обеспечения конфиденциальности, целостности и доступности системы электронных торгов электронная торговая площадка (ЭТП) ЗАО «Сбербанк-АСТ» оснащена эшелонированной системой безопасности.

Одним из ее элементов является система разграничения доступа, которая проводит, в частности, аутентификацию пользователей, а также обеспечивает конфиденциальность их участия в аукционах на ЭТП гос. закупок и других ЭТП, где такая конфиденциальность установлена требованиями ФЗ и нормативными документами.

Аутентификация пользователей проводится по учетной записи (логину) и паролю, либо по сертификату ключа проверки электронной подписи.

Аутентификация по логину и паролю проводится путем вычисления ХЭШ-функции для введенного клиентом пароля и ее сверке с ХЭШ-функцией, хранящейся для данной учетной записи на ЭТП. **Пароли пользователей на ЭТП не хранятся**. Восстановление пароля пользователя по ХЭШ-функции может оказаться возможным путем подбора, если пользователь использовал простой пароль, не соответствующий по сложности требованиям к парольной защите.

Для выполнения юридически значимых операций на ЭТП гос. закупок и ряде других ЭТП ЗАО «Сбербанк-АСТ» используются механизмы аутентификации по сертификату и подписания электронных документов электронной подписью (ЭП). В этом случае подписание и шифрование документов производится на стороне клиента его ключом электронной подписи. **На ЭТП ключ электронной подписи клиента не передается.**

Однако объектом воздействия киберпреступников является не только ЭТП, но и ее клиенты.

2. **Угрозы и риски**

2.1. При пользовании сетью Интернет существуют риски дистанционного хищения с Вашего компьютера конфиденциальной информации, а также дистанционного управления Вашим компьютером.

2.2. Заражение Вашего компьютера вредоносными программами типа Zeus, SpyEye и т.п. приводит к хищению злоумышленниками Ваших электронных ключей (если они не на защищенном ключевом носителе), учетных записей, паролей, персональных данных и т.п. и (или) к дистанционному доступу злоумышленников к Вашему компьютеру, что позволяет злоумышленникам совершать действия от Вашего имени (в том числе с защищенными ключевыми носителями). Это может негативно сказаться не только на состоянии Ваших финансовых счетов, управляемых с зараженного компьютера, но и на других аспектах Вашей деятельности, которые могут представлять для злоумышленников интерес, в том числе на результатах Вашего участия в электронных торгах.

2.3. При заражении вредоносными программами Ваш компьютер может стать членом БОТ-сети и использоваться злоумышленниками для атак на электронную торговую площадку и другие ресурсы сети Интернет. Это может привести к блокированию доступа для Вашего компьютера со стороны атакованных ресурсов (т.н. внесение в «черный список»).

2.4. К блокировке доступа может также привести использование Вами различных средств автоматизации для сканирования сайта ЭТП, а также нелицензионного программного обеспечения, создающих аномальный трафик.

2.5. Клиенту электронной площадки ЗАО «Сбербанк-АСТ» злоумышленниками может быть предложен ложный сайт ЗАО «Сбербанк – АСТ», либо похожий по стилю сайт якобы партнера ЗАО «Сбербанк – АСТ», который предоставляет различные услуги (регистрацию и т.п.).

2.6. Клиент может получать от якобы сотрудников ЗАО «Сбербанк-АСТ» или его партнеров предложения услуг по электронной почте, либо по телефону. Цель такого предложения обычно состоит в получении от клиента его регистрационных данных на сайте ЗАО «Сбербанк – АСТ» - логин, пароль и т.п. (фишинг). **Сотрудники ЗАО «Сбербанк-АСТ» никогда не просят клиентов предоставить свой логин и пароль, либо секретный ключ.**

2.7. Клиент может получать ложные сообщения, якобы от ЗАО «Сбербанк-АСТ», по электронной почте, либо SMS о состоянии (результатах) торгов, рекомендации обращаться за теми или иными услугами в те или иные организации, информацию о необходимости перевода каких-то денежных сумм на указанные в письме счета и т.п.

2.8. Необходимо учитывать риски хищения или несанкционированного использования конфиденциальной информации (пароли, ключи и т.п.) сотрудниками Вашей организации (инсайд).

2.9. Существуют риски потери действительности сертификата ключа проверки электронной подписи (например, если ключ скомпрометирован или владелец уволился, утратил полномочия, Удостоверяющий центр не опубликовал своевременно

список отозванных сертификатов (COC) и т.п.), выхода из строя ключевого носителя или потери доступа к сайту ЭТП.

2.10 Наличие в почтовых сообщениях клиента в адрес ЭТП опасных вложений (исполняемых файлов), ссылок на внешние сайты сомнительной репутации (по базам систем защиты) и рекламы создает риск блокирования этих сообщений системами безопасности ЭТП. Кроме того, при обнаружении в почтовом сообщении клиента вредоносного программного обеспечения может быть блокирован адрес отправителя.

3. Меры информационной безопасности

Для снижения вышеуказанных рисков рекомендуются следующие меры безопасности:

3.1 Организационные меры:

3.1.1. Примите меры по ограничению доступа к компьютерам, используемым для работ с ЭТП.

3.1.2. Не используйте простые пароли. Пароль должен иметь длину не менее 8 символов и использовать **случайную** последовательность букв (в различных регистрах), цифр и спецсимволов. Периодически, а также при подозрении на компрометацию, пароль нужно менять.

3.1.3. Не используйте компьютеры, выделенные для работы с ЭТП, для посещения ненадежных сайтов.

3.1.4. Не устанавливайте на компьютер для работ с ЭТП программы, полученные из ненадежных источников (с нелицензионных дисков или сайтов Интернет, не являющихся официальными сайтами известных разработчиков этих программ).

3.1.5. Для входа в личный кабинет пользуйтесь защищенным протоколом: HTTPS (пример: https://www.sberbank-ast.ru). Контролируйте адрес (URL) и сертификат безопасности сайта.

3.1.6. Не пользуйтесь иными сайтами, в том числе внешне похожими на сайт ЗАО «Сбербанк – АСТ», предлагающими различные услуги в организации и проведении торгов на ЭТП ЗАО «Сбербанк – АСТ» – это фишинг.

3.1.7. Не пользуйтесь услугами лиц, предлагающих оказать содействие в достижении желаемых результатов торгов, либо предоставить конфиденциальную информацию об их участниках – это мошенники.

3.1.8. Для получения информации пользуйтесь официальным сайтом www.sberbank-ast.ru и официальными контактами, размещенными на сайте в разделе «Контакты». Мы не производим информирование клиентов посредством SMS.

3.1.9. 44-ФЗ 2013 г. определяет **конфиденциальность сведений**, содержащихся в заявках на участие в конкурсе до момента открытия доступа к ним в соответствии с установленной процедурой. Клиент должен помнить о том, что при утрате конфиденциальности его участия в электронном аукционе по его вине, он не только нарушает Закон, но и может оказаться объектом воздействия, направленного на достижение третьей стороной желаемых результатов аукциона (уговоры, подкуп сотрудников, угрозы, атаки на технические средства клиента и т.п.). Для снижения этого риска клиент должен, в частности, следить за тем, чтобы раскрывающая его

конфиденциальная информация не была им внесена случайно в открытую часть его заявки на участие в аукционе. К раскрытию участия клиента в конкретном аукционе приводит размещение им в открытой части заявки:

- электронных документов на фирменных бланках клиента;
- электронных документов, раскрывающих клиента по их тексту;
- электронных документов, раскрывающих клиента в атрибутах прикладываемых им файлов, либо имеющих такие же уникальные атрибуты, как и в документах предыдущих аукционов, которые уже раскрыты;
- электронных документов, раскрывающих клиента в удаленных клиентом в ходе их подготовки фрагментах, если эти фрагменты можно восстановить;
- электронных документов, выгруженных клиентом из своей внутренней системы электронного документооборота вместе с электронной подписью (ЭП), которой они там были подписаны и сертификатом ключа проверки этой ЭП.

3.1.10. К раскрытию клиента также приводит использование клиентом **услуг различных компаний и частных лиц** – «знатоков» электронных торгов, предлагающих клиенту подготовку за него документов, настройку компьютера, участие в торгах и предлагающих наделить соответствующими полномочиями своего сотрудника по доверенности клиента. Полученные таким путем полномочия и доступ к информации клиента с большой вероятностью будут использоваться не только в интересах клиента.

3.1.11. Информация о партнерах и области партнерских отношений размещена на сайте ЗАО «Сбербанк-АСТ». **Остальные организации, выдающие себя за партнеров, таковыми не являются.** При работе с партнерами необходимо контролировать соответствие предлагаемых ими услуг области партнерских отношений.

3.1.12. В целях затруднения идентификации злоумышленниками заявки клиента на участие в аукционе по сумме платежа обеспечительного взноса мы рекомендуем переводить сумму не совпадающую с требуемой, а несколько превышающую ее.

3.2. Технические меры:

3.2.1. Компьютер для работ с ЭТП должен быть оборудован лицензионной антивирусной защитой с актуальными антивирусными базами и настроенным персональным межсетевым экраном. На персональном межсетевом экране рекомендуется **запретить доступ ко всем внешним и внутренним сетевым ресурсам**, использование всех протоколов обмена, за исключением фиксированного количества, необходимого для работы (сайты ЭТП, гос. закупок, обновления Windows, Office, антивируса и т.п.).

3.2.2. На программное обеспечение должны регулярно устанавливаться обновления безопасности, выпускаемые его разработчиками.

3.2.3. Периодически (не реже раза в месяц) необходимо проводить полное антивирусное сканирование компьютера, в том числе альтернативным антивирусом. Бесплатную утилиту для одноразового сканирования компьютера альтернативным антивирусом можно скачать, например, с сайта Лаборатории Касперского или Dr.Web.

3.2.4. При получении сертификата ключа проверки ЭП ключ ЭП должен генерироваться Вами или Удостоверяющим центром (реестр авторизованных УЦ http://www.sberbank-ast.ru/SBCAAuthorizeList.aspx) в режиме «без возможности копирования ключевого контейнера» и размещаться на защищенном ключевом носителе, сертифицированном ФСТЭК РФ (ФСБ РФ) – eToken, ruToken и т.п. Остерегайтесь посредников (организаций и физических лиц, не имеющих лицензий ФСБ РФ, но предлагающих помощь в получении ключей и сертификатов). Ключевой носитель должен подключаться к компьютеру только на время работ с ЭТП. В остальное время ключевой носитель должен быть **извлечен из компьютера** и храниться в надежном месте, исключающем доступ посторонних лиц.

3.2.5. На компьютере должны быть отключены функции (службы), используемые для дистанционного доступа (RDP, удаленный помощник), не должны устанавливаться программы удаленного администрирования (RAdmin и т.п.).

3.2.6. Работа в Интернет должна производиться под учетной записью, не имеющей прав локального администратора.

3.2.7. Для набора паролей рекомендуется пользоваться виртуальной клавиатурой.

3.2.8. В нерабочее время компьютер необходимо ВЫКЛЮЧАТЬ.

3.2.9. Клиенту необходимо помнить, что глобальная сеть Интернет НЕ ЯВЛЯЕТСЯ СИСТЕМОЙ ГАРАНТИРОВАННОГО ДОСТУПА и его доступ к ЭТП, может быть потерян в самый неподходящий момент, как вследствие неисправностей, так и действий злоумышленников на любом участке прохождения его трафика до ЭТП. При этом доступ к другим Интернет-ресурсам может сохраниться.

3.2.10. Не следует надеяться на устойчивость связи мобильного Интернет (Sky Link, Yota, 3G-модемы операторов сотовой связи и т.п.). Она зависит от многих факторов, в том числе от текущей электромагнитой обстановки.

3.2.11. В случае потери доступа к ЭТП нужно:

- задокументировать ситуацию: сделать скриншоты, показывающие недоступность ЭТП и доступность других Интернет-ресурсов;
- установить внешний IP своего компьютера. Это можно сделать на ряде сайтов Интернет, например, http://ipgeobase.ru или http://2ip.ru/;
- при возможности проверить доступность ЭТП с другого компьютера и другого IP-адреса. Если у Вас динамический IP, то отключиться от Интернет и подключиться опять. При этом IP может измениться и доступность ЭТП тоже;
- полученные материалы прислать в службу технической поддержки ЭТП.

Если с ЭТП получен ответ, что Вашего IP в черном списке нет, то для установления причины отсутствия доступа потребуется дополнительная диагностика. В целях ее проведения рекомендуется заблаговременно (т.е., когда ЭТП доступна) задокументировать маршрут прохождения Вашего трафика на ЭТП. Для этого в командной строке (вход в режим командной строки по команде CMD) набрать:

tracert www.sberbank-ast.ru > C:\trace.txt

Далее сохранить файл C:\trace.txt в надежном месте в качестве эталонного. В случае потери доступа к ЭТП получить новый файл trace.txt и сравнить с эталонным или прислать его по электронной почте в службу технической поддержки ЭТП.

3.2.12. Для снижения рисков потери доступа к ЭТП во время аукциона (в том числе вследствие действий злоумышленников) рекомендуется заблаговременно подготовить к работе с ЭТП резервный компьютер, подключенный к сети Интернет через другого (альтернативного) провайдера. Во время аукциона быть в готовности в течение 5 минут перейти на резервный компьютер.

3.2.13. Для снижения рисков, связанных с неисправностью носителя ключа электронной подписи или проверкой действия сертификата электронной подписи на ЭТП рекомендуется иметь два ключа электронной подписи на двух разных носителях и, соответственно, два сертификата, полученные в двух разных удостоверяющих центрах.

3.2.14. Для снижения рисков потери доступа к сайту во время DDoS-атак на ЭТП, мы рекомендуем клиентам иметь статический IP-адрес. Чтобы снизить риск DDoS-атаки на свой компьютер, клиент свой статический IP должен хранить в тайне.

3.2.15. Не откладывайте свои операции на ЭТП на последний момент. В последний момент может что-нибудь случиться, и Вы не успеете отреагировать (повторить операцию, перейти на резервный компьютер и т.п.).

3.2.16. Мы не рекомендуем клиентам скрывать свой истинный IP-адрес, используя вход на сайт ЭТП через анонимные прокси-серверы, TOR и т.п. системы, так как это повышает риск блокировки доступа системами безопасности ЭТП.

3.2.17. При выезде зарубеж необходимо учитывать, что доступ на ЭТП из ряда «неблагополучных» (с точки зрения вредоносной Интернет-активности) районов Мира может оказаться блокирован: Китай, Индия, Юго-Восточная Азия, Африка, Южная Америка, ряд арабских стран. Выходить на ЭТП из таких районов мы рекомендуем через Ваш офис в России (например, используя его как прокси и т.п.).

3.2.18. Для снижения влияния случайностей (неисправность компьютера, потеря доступа к ЭТП и т.п.) на Ваше участие в торгах мы также предлагаем клиентам использовать штатный функционал ЭТП – аукционного робота. Робот будет торговаться за Вас до заблаговременно заданного Вами лимита снижения начальной максимальной цены контракта, а Вы можете наблюдать за ним и, если в ходе аукциона потребуется, остановить его и завершить аукцион в ручном режиме. Если же Вы по каким-либо техническим причинам потеряли связь с ЭТП, Ваш робот завершит аукцион сам.

3.2.19. При переписке с ЭТП по электронной почте не следует включать в сообщение ссылки перехода на сайты (если они не имеют отношения к сути излагаемого вопроса), исполняемые файлы, рекламу, так как такое письмо до получателя может не дойти.

4. Заключение

Выполнение рекомендаций данной инструкции в полном объеме не всегда удобно и не для всех просто. Каждый клиент сам решает, в какой степени он будет им следовать исходя из тех рисков, которые он для себя считает допустимыми.