РЕКОМЕНДАЦИИ
по информационной безопасности при работе в системе дистанционного банковского обслуживания «Банк-Клиент»

1. Термины и определения.

Защитная мера - сложившаяся практика, процедура или механизм, которые используются для уменьшения Риска нарушения Информационной безопасности в Системе ДБО.

Злоумышленник - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

Злоумышленные действия – любые действия, совершаемые Злоумышленником в Системе ДБО.

Информационная безопасность - безопасность, связанная с Угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

Инцидент - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы Информационной безопасности

Обработка риска нарушения информационной безопасности - процесс выбора и осуществления Защитных мер, снижающих Риск нарушения Информационной безопасности, или мер по переносу, принятию или уходу от Риска

Риск - мера, учитывающая вероятность реализации Угрозы и величину потерь (ущерба) от реализации этой Угрозы.

Риск нарушения информационной безопасности - Риск, связанный с Угрозой Информационной безопасности.

Угроза - опасность, предполагающая возможность потерь (ущерба).

2. Настоящие Рекомендации определяют Защитные меры по обработке Рисков нарушения Информационной безопасности при использовании Клиентами Системы ДБО.

3. При использовании Системы ДБО необходимо учитывать, что:

- сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из сети Интернет;
- гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;

– расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы. В целях проведения расследования пострадавшая сторона должна предоставить в распоряжение следственных органов компьютер, который использовался для доступа в Систему ДБО, для проведения экспертизы.

4. Не сообщайте посторонним лицам, а также кому бы то ни было через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, контактные и учетные данные, так как эти данные могут быть перехвачены Злоумышленником и использованы для получения доступа к Вашим счетам.

5. Не используйте функцию запоминания логина и пароля в браузерах.

6. Не используйте одинаковые логин и пароль для доступа к различным системам.

7. Всегда явным образом завершайте сеанс работы с Системой ДБО, используя пункт меню «Выход».

8. В случае если доступ к Системе ДБО осуществляется с использованием постороннего компьютера, не рекомендуется сохранять на нем идентификационные данные и другую информацию, а после завершения всех операций нужно убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному персональному компьютеру обязательно смените логин и пароль.

9. Если Вы получили на электронную почту письмо с просьбой обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), перезвоните в Банк по телефону (39543) 37-0-37 и сообщите о письме или перешлите его на адрес avtomat@greencombank.ru. Банк никогда не просит передать данные по электронной почте. Обновление данных осуществляется только сотрудником Банка в присутствии представителя Клиента предъявившего документ, удостоверяющий личность. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах и не отвечайте на них.

10. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть ваши идентификационные данные для входа в Систему ДБО и ключи ЭЦП/ЭП.

11. Регулярно, не реже одного раза в месяц, производите смену пароля.

12. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >.

13. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

14. Не позволяйте третьим лицам производить за Вас генерацию ключей ЭЦП/ЭП.

15. Присоединяйте ключевой носитель ЭЦП/ЭП к компьютеру непосредственно перед началом работы с Системой ДБО. По окончании работы извлекайте ключевой носитель из компьютера.

16. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что Вы несете уголовную ответственность за пользование нелицензированным программным обеспечением в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

17. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения, установленного на компьютере, производите установку обновлений операционной системы и обновляйте антивирусные базы. В случае обнаружения вирусов (вредоносного программного обеспечения) на компьютере, после его удаления незамедлительно смените логин и пароль в Системе ДБО и произведите замену ключей ЭЦП/ЭП.

18. Регламентируйте порядок использования компьютера, с которого осуществляется взаимодействие с Системой ДБО, в том числе список лиц и порядок доступа к компьютеру. Не рекомендуется использовать указанный компьютер для доступа к посторонним сайтам.

19. Не устанавливайте на компьютере, который используется для взаимодействия с Системой ДБО, постороннее программное обеспечение, например программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы могут передавать информацию о содержимом просматриваемых страниц посторонним лицам.

20. Не запускайте на своем компьютере программы, полученные из не заслуживающих доверия источников.

21. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

22. Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам.

23. Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности.

24. В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов ЗАО «Гринкомбанк», просьба сообщить об этом по электронной почте avtomat@greencombank.ru.

25. Поддерживайте свою контактную информацию в Системе ДБО в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться. В целях оперативного реагирования на Злоумышленные действия пользуйтесь услугой дополнительного информирования.

26. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе ДБО, незамедлительно смените логин и пароль, сообщите об инциденте в Банк по телефону (39543) 37-0-37 и произведите смену ключей ЭЦП/ЭП.

27. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо в максимально короткий срок отозвать сертификат ЭЦП/ЭП и оформить заявление в операционном подразделении Банка в свободной форме, содержащее максимально подробное описание инцидента, для инициирования расследования. Для проведения расследования необходимо по согласованию с сотрудником отдела автоматизации, программного и технического сопровождения передать в Банк файлы протоколов, подтверждающие установку обновлений операционной системы персонального компьютера и антивирусного программного обеспечения, и в течение 5 (пяти) рабочих дней представить в подразделение Банка для снятия копий документы, подтверждающие факт законного приобретения операционной системы и антивирусного программного обеспечения, а также копию договора об оказании услуг по предоставлению доступа в сеть интернет или иного документа, удостоверяющего факт заключения подобного договора (квитанция, чек, счет и тому подобные) и иные документы, которые Клиент сочтет необходимыми для рассмотрения претензии по существу. В случае невозможности представления необходимых файлов и документов, об этом делается соответствующая запись на заявлении с указанием причины. Необоснованный отказ в предоставлении требуемых документов может являться основанием для отказа в удовлетворении заявленных Клиентом требований. **Решение об обращении в правоохранительные органы Клиент принимает самостоятельно**.