Правила информационной безопасности
при использовании клиентами БАНКА «МНХБ» ПАО
систем дистанционного банковского обслуживания

1. Общие положения

1. Термины и определения:

Банк - «Московский Нефтехимический банк» публичное акционерное общество (БАНК «МНХБ» ПАО), а также его Отделения и Филиал

Система ДБО - система дистанционного банковского обслуживания корпоративных клиентов «АСЭД iBank2» или иная Система ДБО, предоставленная Банком

Клиент - юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством РФ порядке частной практикой, заключающие / заключившие с Банком Договор банковского счета с возможностью использования систем дистанционного банковского обслуживания

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

Угроза - опасность, предполагающая возможность потерь (ущерба)

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

Информационная безопасность (ИБ) - 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)

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

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

Риск нарушения ИБ - риск, связанный с Угрозой ИБ

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

Электронная подпись (ЭИ) - электронный аналог собственноручной подписи уполномоченного должностного лица Клиента, в виде данных, добавленных к тексту электронных документов и полученных в результате ее криптографического преобразования, обеспечивающий возможность контроля целостности и подтверждения подлинности электронных документов. Электронная подпись позволяет подтвердить ее принадлежность зарегистрированному в Банке Владельцу электронной подписи

Персональный аппаратный криптопровайдер (ПАК) - USB-токен или смарт-карта «iBank2Key» - защищенное хранилище ключей Электронной подписи на отчуждаемом носителе

2. «Правила информационной безопасности при использовании клиентами БАНКА «МНХБ» ПАО систем дистанционного банковского обслуживания» (далее - Правила) разработаны в соответствии с:

- Федеральным законом от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе»,
- Стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»,
- Международными стандартами ISO 27001:2005 и ISO 17799:2005,

- Положением Банка России от 09.06.2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»,
- Политикой информационной безопасности БАНКА «МНХБ» ПАО,
- Иными законодательными и нормативными актами, регулирующими вопросы информационной безопасности.

1. Правила являются обязательными к исполнению всеми Клиентами, использующими в работе с Банком Системы ДБО.
2. Правила определяют Защитные меры по обработке Рисков нарушения ИБ при использовании Клиентами Системы ДБО. При этом Клиент обязан 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 обеспечения 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.

1. Ограничение ответственности Банка

1.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему ДБО, Клиент использует технические и программные средства, не принадлежащие Банку, Банк не несет ответственности за любые, в том числе Злоумышленные, действия третьих лиц в отношении и / или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.

1.2. За пользование нелицензированным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 УК РФ.

1.3. Срок для предъявления Банку претензий по услугам, оказанным с использованием Системы ДБО, составляет 10 календарных дней с даты осуществления операции. По каждой опротестовываемой операции оформляется отдельная претензия. Решение по претензии принимается Банком в течение 30 (тридцати) рабочих дней со дня подачи заявления в офисе Банка и предоставления Клиентом необходимого пакета документов, в соответствии с разделом 4 настоящих Правил.

1.4. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы ДБО. Содержимое журнала Системы ДБО используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования Злоумышленных действий.

3. Защитные меры

Банк обращает внимание Клиентов на то, что окончательное решение об использовании предлагаемых Банком в разделе 3 настоящих Правил Защитных мер принимает Клиент.

3.1. Защитные меры общего характера:

- 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,
- 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,
- используйте и оперативно обновляйте специализированное ПО для защиты информации - антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.,
- используйте и оперативно обновляйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений;
- соблюдайте правила безопасной работы в Интернете, а именно: не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители, не читайте подозрительных электронных писем, максимально ограничьте использование Интернет-пейджеров (ICQ и пр.) и т.п.,
- не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников,
- используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации,

3.2. Защитные меры при использовании логинов и паролей:

- никогда не записывайте логины и пароли на бумаге, мониторе или клавиатуре,
- не используйте одинаковые логин и пароль для доступа к различным системам,
- при составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < > . Настоятельно рекомендуется использовать специализированные программы-генераторы паролей,
- не используйте в качестве пароля имена, памятные даты, номера телефонов.

3.3. Защитные меры при работе с электронной почтой (особенно если вы используете открытые почтовые серверы, типа mail.ru, yandex.ru и т.д.):

- если Вы получили на электронную почту письмо, содержащее просьбу обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе - сайт Банка), перезвоните в Службу технической поддержки по телефону (495) 223-01-01 доб.1110, 1212 и сообщите о письме или перешлите его на адрес dbo@mnhb.ru. **Банк никогда не просит передать конфиденциальные данные по электронной почте.** 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,
- 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 пароли к ключам ЭП.

3.4. Защитные меры при работе с Системой ДБО:

- четко 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),

- соблюдайте регламент ограниченного физического доступа к компьютеру, с которого осуществляется взаимодействие с Системой ДБО, рекомендуется иметь утвержденный список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютерам, с которых осуществляется работа в Системе ДБО,
- 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 передают информацию о содержимом просматриваемых страниц посторонним лицам,
- не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам,
- перед вводом своего пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности. В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов БАНКА «МНХБ» ПАО, просьба сообщить об этом по электронной почте dbo@mnhb.ru.
- не пользуйтесь Системой ДБО в Интернет-кафе, а так же там, где вы не уверены в безопасности компьютеров и доверенности среды исполнения,
- регулярно проверяйте, встроенную в систему Интернет банк-клиент страничку «Сеансы работы», которая содержит информацию обо всех входах в Систему ДБО.
- поддерживайте свою контактную информацию в Системе ДБО в актуальном состоянии для того, чтобы в случае необходимости с вами можно было оперативно связаться,
- 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,
- присоединяйте Персональный аппаратный криптопровайдер (ПАК) к компьютеру непосредственно перед началом работы с Системой ДБО, по окончании работы извлекайте ПАК из компьютера,
- не допускается хранить ПАК в местах, где к нему может получить доступ кто-либо, кроме Вас, отчуждаемый носитель с хранилищем ключей необходимо тщательно оберегать от несанкционированного доступа,
- в случае если доступ к Системе 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 пароль доступа к ключу ЭП,
- регулярно, не реже одного раза в месяц, производите смену пароля доступа к ключам ЭП,
- не позволяйте третьим лицам производить за вас генерацию ключей ЭП,
- при увольнении ответственного сотрудника, имевшего доступ к секретному ключу ЭП, обязательно сообщите в Банк (по телефонам, указанным в п. 3.3. Правил) и заблокируйте ключ ЭП,
- при возникновении любых подозрений на компрометацию (кражу ПАК) секретных ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) - обязательно сообщить в Банк и заблокировать ключи ЭП,

- в случае обнаружения вирусов (вредоносного программного обеспечения) на компьютере, после его удаления незамедлительно смените логин и пароль в Системе и произведите смену ключей ЭП,
- Банк настоятельно рекомендует Клиентам использовать встроенный в Систему ДБ О механизм дополнительного подтверждения платежных поручений одноразовыми паролями с привязкой реквизитам платежа (дополнительно к механизму ЭП), посредством использования Устройства, генерирующего одноразовые пароли (УГОП).

4. Оповещение Банка о подозрительных (несанкционированных) действиях в Системе ДБО

4.1. При обнаружении подозрительных действий (признаков подозрительных действий), совершенных от Вашего имени в Системе ДБО, незамедлительно смените пароль, сообщите об инциденте в Службу технической поддержки и произведите смену ключей ЭП.

4.2. При обнаружении несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо в максимально короткий срок отозвать сертификат 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 со Службой технической поддержки передать в Банк:

- файлы протоколов, подтверждающие установку обновлений операционной системы персонального компьютера и антивирусного программного обеспечения,
- в течение 5 (пяти) рабочих дней представить в операционное подразделение Банка для снятия копий документы, подтверждающие факт законного приобретения операционной системы и антивирусного программного обеспечения,
- копию договора об оказании услуг по предоставлению доступа в сеть интернет или иного удостоверяющего факт заключения подобного договора документа (квитанция, чек, счет и тому подобные),
- 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.**