Требования и рекомендации по обеспечению информационной безопасности Рабочего Места КЛИЕНТА в системе «iBank 2»

1. Общие положения

1.1. Данные методические рекомендации разработаны на основе:

- «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 февраля 2001 года №152**;**
- «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005г. № 66;
- эксплуатационной документации:
  - ✓ на USB-токен (смарт-карту);
  - ✓ на криптобиблиотеки, поддерживаемые разработчиком системы «iBank2» (состав криптобиблиотек, имеющих на данный момент времени сертификаты ФСБ и рекомендуемых для работы предложен на сайте банка);
- технической документацией на систему «iBank 2» (далее по тексту Система).

1.2. Информационная безопасность Рабочего Места КЛИЕНТА системы «iBank 2» (далее по тексту РМ) должна обеспечиваться с использованием комплексных (организационных, административных, технических и программных) мер и средств.

1.3. С целью обеспечения безопасности информации:

- руководством КЛИЕНТА должен быть утвержден список пользователей и администраторов, допускаемых к работе на РМ, с закреплением за каждым пользователем конкретных функций и полномочий;
- руководством КЛИЕНТА должен быть назначен сотрудник ответственный за обеспечение безопасности РМ;
- пользователи РМ должны пройти обучение правилам эксплуатации согласно документации, на Систему и быть ознакомлены с настоящими методическими рекомендациями;
- оборудование РМ должно размещается в служебных помещениях, для которых обеспечен режим ограниченного доступа;
- программное обеспечение РМ и носители ключевой информации должны быть защищены от несанкционированного доступа (НСД).

1.4. Использование персонального аппаратного криптопровайдера с неизвлекаемыми ключами ЭП (USB токена) защищает секретные ключи от копирования, но не освобождает от выполнения изложенных требований.

1.5. Обеспечение безопасной среды исполнения на компьютере клиента - это задача, которую может и должен решать только клиент. Банк не может за клиента решить эту задачу, поскольку объект защиты (компьютер) находится в полном распоряжении клиента.

2. Требования по защите ПО РМ КЛИЕНТА от несанкционированного доступа (НСД)

2.1. Защита ПО РМ КЛИЕНТА и носителей ключевой информации от несанкционированного доступа осуществляется с целью исключения возможностей:

- появления в компьютерах, на которых установлены средства Системы, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию ПО Системы, либо на перехват информации, в том числе паролей секретных ключей;
- внесения несанкционированных изменений в технические и программные средства Системы, а также в их состав;
- внесения несанкционированных изменений в ЭД.

2.2. Программное обеспечение автоматизированного рабочего места приема/передачи платежных электронных документов Системы рекомендуется устанавливать на отдельный, специально выделенный для этих целей персональный компьютер, на котором будет ограничен список доступных для соединения адресов, в частности, только сервера банка, а также производителей антивирусного продукта, Java, ОС для своевременного обновления указанного ПО. **Должна быть обеспечена в обязательном порядке защита данного компьютера от сетевых атак и антивирусная защита.**

2.3. В целях защиты РМ КЛИЕНТА от несанкционированного доступа на РМ рекомендуется установить программно-аппаратный комплекс защиты от несанкционированного доступа.

2.4. Рекомендуется сформировать с помощью комплекса защиты от НСД функционально замкнутую среду, обеспечивающую контроль целостности ПО и допускающую работу пользователей строго в рамках, предоставляемых им возможностей и полномочий. Защите подлежат системные и загрузочные файлы, а также файлы, связанные с работой средств криптографической защиты информации (СКЗИ).

2.5. На ЭВМ не должны устанавливаться средства разработки ПО и отладчики.

2.6. Следует принять меры, препятствующие несанкционированному вскрытию системных блоков персональных компьютеров, входящих в состав РМ КЛИЕНТА.

2.7. Права администратора программно-аппаратных средств защиты от НСД предоставляются сотруднику, ответственному за обеспечение безопасности РМ. Указанный сотрудник формирует права доступа для каждого пользователя Системы, участвующего в приеме-передаче ЭД, формировании ЭД и использовании носителей ключевой информации.

2.8. Для защиты компьютеров РМ от НСД также должны использоваться штатные возможности операционной системы.

3. Требования по организации хранения и использования носителей ключевой информации

3.1. Клиент должен самостоятельно генерировать криптографические ключи.

3.2. Носители ключевой информации должны храниться только у тех лиц, которым они принадлежат.

3.3. Порядок хранения и использования носителей ключевой информации с ключами ЭП должен исключать возможность несанкционированного доступа к ним.

3.4. Список лиц, имеющих доступ к носителям ключевой информации, определяется приказом или распоряжением руководства КЛИЕНТА, согласно закрепленными за ними функциями и полномочиями.

3.5. Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

3.6. Для хранения носителей ключевой информации должны устанавливаться надежные металлические сейфы.

3.7. По окончании рабочего дня, а также вне времени сеансов связи с Банком, носители ключевой информации должны храниться в сейфе.

3.8. Хранение носителей ключевой информации допускается в одном сейфе с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.

3.9. Не разрешается:

- передавать носители ключевой информации лицам, к ним не допущенным;
- выводить ключи ЭП (секретные) на дисплей или принтер;
- вставлять носитель ключевой информации в считывающее устройство компьютера в режимах, не предусмотренных функционированием РМ, а также в считывающие устройства других компьютеров;
- оставлять носитель ключевой информации без присмотра на рабочем месте;
- записывать на носитель ключевой информации посторонние файлы.

4. Практические рекомендации по защите РМ от несанкционированного доступа

4.1. Рекомендуется полностью блокировать сетевой доступ к ресурсам РМ (в том числе и удаленный вход в сеть) с других рабочих станций локальной сети и в особенности из внешних сетей. С этой целью рекомендуется установить и настроить соответствующим образом персональный межсетевой экран.

4.2. Рекомендуется ограничить использование сети Интернет пользователями РМ, т.е. ограничить список доступных для соединения адресов, например, разрешить только соединение с сервером банка. С этой целью также лучше всего использовать установленный персональный межсетевой экран.

4.3. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов.

4.4. На компьютере, через который выполняется работа в Системе, необходимо регулярно устанавливать обновление операционной системы (желательно в автоматическом режиме).

4.5. Пользователи РМ, работающие с системой не должны иметь прав администратора, с целью ограничения возможностей установки под этими учетными записями программного обеспечения на компьютере. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.

4.6. Пользователи РМ, должны быть в обязательном порядке проинструктированы по вопросам соблюдения основных требований безопасности, и в особенности по вопросам использования антивирусных программ.

4.7. Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.

4.8. Рекомендуется ограничить или полностью отказаться от приема внешней (из Сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.

4.9. На компьютере должна быть установлена только одна ОС.

4.10. Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. отключить загрузку с дискет, CD/DVD приводов, USB flash дисков, сетевую загрузку и т.п.

4.11. Доступ к изменению настроек BIOS должен быть защищен паролем.

4.12. Пользователям операционной системы должны быть назначены пароли.

4.13. Длина используемых паролей должна составлять не менее шести символов. Срок действия паролей должен быть ограничен. Сложность пароля должна быть достаточной, чтобы исключить возможность подбора пароля в ручном или автоматизированном режимах.

4.14. Рекомендуется опечатать системный блок компьютера для предотвращения его несанкционированного вскрытия.

4.15. Для ограничения доступа к компьютеру, проверки целостности используемого ПО, рекомендуется установить и настроить на компьютер программно-аппаратный комплекс защиты от НСД («Аккорд», «Соболь» и т.п.).

4.16. Подключать носители ключей ЭП (USB-токен, смарт-карту) необходимо только непосредственно при работе с системой в моменты выполнения операций подписания или обмена с Банком, по завершении операции необходимо извлечь данный носитель. Не подключайте носители с ключевой информаций к другим компьютерам.

4.17. Не рекомендуется подключать к РМ внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

4.18. При подключении к системе «iBank2» на сервере банка следует убедится, что тип соединения «https», а SSL сертификат подлинен и выдан ibank.dvbank.ru.

4.19. При обнаружении подозрительной активности на компьютере с установленной Системой (самопроизвольные движения мышью, открытие/закрытие окон, набор текста) следует немедленно выключить компьютер и сообщить в Банк о возможной попытке несанкционированного доступа к счету(-ам).

5. Общие требования по учету СКЗИ

5.1. Необходимо вести Журнал поэкземплярного учета СКЗИ и ключевых носителей к ним.

5.2. Уничтожение секретных ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

5.3. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия ключи шифрования и ЭП со всех магнитных носителей не позднее чем через десять дней после момента вывода ключей из действия. Об уничтожении ключей делается соответствующая запись в Журнале учета.

5.4. Порядок гарантированного уничтожения ключа ЭП в персональном аппаратном криптопровайдере описан в документе «Руководство по работе с USB токенами.

5.5. Уничтожение (утилизация) персонального аппаратного криптопровайдера осуществляется путем физического разрушения его внутренних микросхем.

5.6. В случае уничтожения (утилизации) USB-токена должен быть составлен акт по форме, установленной банком.

6. Дополнительные меры безопасности в системе «iBank 2».

6.1. Необходимо помнить о риске хищения ключей (копирование ключей на отчуждаемом носителе) и возможности несанкционированного использования ключа на персональном аппаратном криптопровайдере (случайное оставление ключевого носителя, подбор ключа к сейфу для хранения токена, удаленное подключение злоумышленника к компьютеру). Для противодействия этим рискам необходимо начинать каждый сеанс связи с анализа времени последнего сеанса работы в системе, для того, чтобы убедиться, что последний сеанс связи совершен Вами, а не злоумышленником.

6.2. В случае использования ключей на отчуждаемых носителях рекомендуется включение режима, ограничивающего доступ в систему «iBank 2» с определенного IP адреса. Для получения формы (бланка) заявления на включение IP- фильтрации – обращайтесь к обслуживающему Вас менеджеру.

6.3. Использовать возможностью многофакторной аутентификации с использованием одноразовых паролей.

6.4. Использовать возможностью дополнительного подтверждения совершения операций с использованием одноразовых паролей.