Банк развития и модернизации промышленности

Требования и рекомендации по обеспечению информационной безопасности при работе в системе «IBank2»

1 Требования по обеспечению информационной безопасности

1.1 Организационные меры

- Рабочее место (РМ) , с которого осуществляется работа в системе «IBank2», должно размещаться в служебных помещениях, для которых обеспечен режим ограниченного доступа.
- Доступ к РМ должен предоставляться лицам, наделенным соответствующими полномочиями.
- 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 ответственный за обеспечение безопасности РМ
- Доступ посторонних лиц в помещение с РМ должен быть ограничен и осуществляться только под контролем уполномоченных лиц.
- Пользователи РМ должны быть в обязательном порядке проинструктированы по вопросам соблюдения требований безопасности.

1.2 Требования по защите АРМ

- На РМ должно быть установлено только лицензионное ПО
- Установленное на РМ ПО должно своевременно обновляться
- На РМ в обязательном порядке должно быть установлено лицензионное антивирусное ПО с ежедневным обновлением .
- На РМ должен быть активирован персональный сетевой экран, разрешающий доступ с РМ только к доверенным ресурсам сети. Сетевой доступ к ресурсам РМ (в том числе и удаленный вход) с других станций сети и в особенности из внешних сетей.
- Использование сети Интернет пользователями РМ должно быть ограничено только соединениями с серверами Банка.
- На РМ не должно быть установлено ПО для разработки и отладки программ.
- Должны быть приняты меры, препятствующие несанкционированному вскрытию системного блока РМ.
- Гостевая учетная запись на РМ должна быть заблокирована.
- Пользователи РМ, работающие с системой не должны иметь прав администратора. Доступ к файловым ресурсам компьютера должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.
- На РМ должна быть установлена только одна операционная система.

- На РМ должен быть исключен режим автоматического входа пользователя в операционную систему при ее загрузки.
- Средствами BIOS должна быть исключена возможность загрузки операционной системы, отличной от установленной на жестком диске (должны быть отключены загрузка с дискет, CD\DVD приводов, USB flash дисков, сетевая загрузка и т.д.)
- Доступ к BIOS должен быть защищен паролем.
- В случае обнаружения на РМ незарегистрированных программ, вирусов, нарушений целостности операционной системы, работа должна быть прекращена, а в Банк направлено уведомление о компрометации ключей для их блокировки.

1.3 Требования к эксплуатации АРМ

- На РМ еженедельно должна выполняться полная антивирусная проверка
- При возникновении подозрения на вирусную активность или при обнаружении вирусов на РМ откажитесь от работы на РМ до полного восстановления его работоспособности.
- Не подключайте к РМ никакие отчуждаемые носители (дискеты, компакт-диски, USB-накопители , мобильные телефоны и т.д.)
- При работе с электронной почтой не открывайте письма от неизвестных отправителей.
- При каждом подключении к серверу банка проверяйте адрес страницы. Адрес должен соответствовать https:\\ibank.bankrmp.ru. Web-сайт интернет-банкинга Банка РМП (ПАО) защищен сертификатом Хостинг-центра. Если, при открытии сайта, возникает предупреждение об ошибке в сертификате безопасности, то необходимо немедленно покинуть страницу и сообщить об этом персоналу Банка.
- Никогда не отвечайте на письма, в которых от имени Банка или иных адресатов Вас просят предоставить какую-либо информацию, связанную с работой в системе «IBank2». Никогда не следуйте по ссылкам в таких письмах, т.к. скорее всего вы попадете на сайт мошенников.
- В случае обнаружения ложного Web-сайта интернет-банкинга, или получения от имени Банка подозрительно электронного сообщения, незамедлительно сообщите об этом персоналу Банка.
- При работе в Интернет никогда не давайте согласия на установку каких-либо дополнительный программ.
- Не оставляйте ключевые носители и USB-токены в компьютере после окончания работы в системе «IBank2»

1.4 Требования по использованию и хранению ключевой информации

- КЛИЕНТ должен самостоятельно генерировать криптографические ключи
- Носители ключевой информации должны храниться у тех лиц, которым они принадлежат.
- Порядок хранения и использования носителей ключевой информации с секретными ключами должен исключать возможность несанкционированного доступа к ним.
- Категорически запрещается сохранять ключевые файлы (файлы ключей ЭП) на жестком диске компьютера
- Во время работы с носителями ключевой информации доступ посторонним к ним должен быть исключен
- По окончании рабочего дня, а так же вне времени сеансов с Банком, носители ключевой информации должны храниться в металлических сейфах

- Не разрешается:
  - ❖ Передавать носители ключевой информации лицам, к ним не допущенным
  - ❖ Выводить секретные ключи на печать или экран монитора
  - ❖ Подключать носители ключевой информации к другим компьютерам и устройствам
  - ❖ Записывать на носители ключевой информации посторонние файлы

2 Рекомендации по обеспечению информационной безопасности

- Рекомендуется ограничить или полностью отказаться от работы с электронной почтой на РМ.
- Рекомендуется с помощью персонального межсетевого экрана запретить на РМ все входящие и исходящие ip-пакеты, за исключением UDP-трафика с DNS-сервером и исходящих TCP- соединений с банковскими web-серверами.
- Регулярно проверяйте РМ на наличие вирусов.
- При кратковременном отсутствии на рабочем месте заблокируйте РМ (средствами операционной системы) и уберите ключевые носители в сейф.
- Избегайте подключений к сомнительным сайтам, а так же ресурсам, маскирующимся под известные кредитные организации.
- В работе используйте надежные, сложные пароли, содержащие различные буквы, цифры и спецсимволы (например, знаки препинания), а так же сочетания заглавных и строчных букв. Не записывайте и никому не сообщайте свои пароли.
- Рекомендуется для хранения ключевых файлов использовать USB-токен.
- В случае, если РМ вышло из строя (не включается, виден «синий» экран) – незамедлительно свяжитесь с банком и выполните блокировку ключей – возможно выход РМ из строя является следствием вирусной атаки, цель которой – лишить вас возможности оперативно отслеживать состояние вашего счета.