Рекомендации Клиенту для обеспечения безопасности информации при использовании системы «Интернет-банк» ПАО «РосДорБанк».

При работе с системой «Интернет-банк», Клиент в обязательном порядке должен соблюдать следующие рекомендации:

1. Рекомендации по защитным мерам для ПЭВМ [1]

1.1. Для работы с системой «Интернет-банк» рекомендуется использовать отдельный компьютер, доступ к которому имеют только лица, осуществляющие платежи в системе «Интернет-банк».

1.2. Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB-flash дисков, загрузка по сети и т.п.

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

1.4. ПЭВМ с системой «Интернет-банк» по окончании рабочего дня рекомендуется выключать.

1.5. На ПЭВМ с установленной системой “Интернет-банк» должна быть установлена только одна операционная система.

1.6. Для работы с системой «Интернет-банк» следует устанавливать операционные системы, которые поддерживаются производителем и для которых выходят регулярные обновления. Использование ОС, поддержка которых прекращена (Windows XP, Windows 7, Windows 8) запрещено.

1.7. Не рекомендуется подключать к ПЭВМ с установленной системой “Интернет-банк» внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

1.8. На компьютере, с которого осуществляется работа в системе «Интернет-банк, необходимо использовать только лицензионное системное и прикладное ПО.

1.9. На ПЭВМ следует устанавливать только то программное обеспечение, которое необходимо и достаточно для выполнения поставленных задач.

1.10. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное ПО (например, Kaspersky, Dr.Web, ESET NOD 32).

1.11. Рекомендуется своевременно проводить обновления системного и прикладного ПО.

1.12. Следует принять меры, препятствующие несанкционированному вскрытию системных блоков ПЭВМ с установленной системой «Интернет-банк».

1.13. Рекомендуется полностью блокировать сетевой доступ к ресурсам ПЭВМ с установленной системой «Интернет-банк».

1.14. На ПЭВМ с установленной системой “Интернет-банк» рекомендуется ограничить использование сети Интернет пользователями системы «Интернет-банк», т.е.

[1] **ПЭВМ –** стационарный компьютер или портативный ноутбук, используемый для работы в системе «Интернет-Банк»

ограничить список доступных для соединения адресов, например, разрешить только соединение с сервером системы «Интернет-банк» (https//corp.rdb.ru/).

1.15. Категорически запрещено:

- посещать социальные сети (Например, ВКонтакте, Одноклассники, Facebook и др.), и другие ресурсы, не связанные с должностными обязанностями работника;
- устанавливать и использовать программы мгновенного обмена сообщениями (Например, ICQ, QIP, Mail.ru agent, Miranda);
- устанавливать и использовать ПО для облачного хранения данных (Например, GoogleDisk, YandexDisk, DropBox, Mail cloud и др.);
- устанавливать и использовать программы, обеспечивающие голосовую и видео связь (Skype, Viber, Microsoft Lync и т.п.);
- устанавливать, запускать, использовать на ПЭВМ с установленной системой “Интернет-банк», ПО для удаленного управления (Например, RDP, TeamViewer, Radmin, Ammyy Admin др.).

1.16. Вся получаемая электронная почта должна проверяться антивирусными средствами.

1.17. Пользователи системы «Интернет-банк», работающие с системой не должны обладать правами администратора на ПЭВМ с установленной системой «Интернет-банк», с целью ограничения возможностей установки под этими учетными записями программного обеспечения на ПЭВМ. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.

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

1.19. Крайне не рекомендуется использовать для доступа к системе “Интернет-банк» общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее).

2. Рекомендации по парольной защите

Учетные записи операционной системы с установленной системой “Интернет-банк» должны быть защищены паролями с учётом следующих параметров:

2.1. Длинна пароля должна быть не менее 8 символов.

2.2. В пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) символы, цифры, а также специальные символы (например, #, %, ^, * и т.п.).

2.3. В качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

2.4. В качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;

2.5. Пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля.

2.6. При смене пароля новый пароль не должен совпадать с ранее используемыми паролями.

2.7. Запрещено произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли доступа к ПЭВМ и системе “Интернет-банк» (например, на мониторе компьютера, под клавиатурой, на столе, в записной книжке и т.п.).

2.8. Запрещено: использовать стандартные пароли доступа к системе «Интернет-банк» т.е., те, которые назначены по умолчанию производителем/разработчиком, они должны быть незамедлительно изменены.

2.9. Блокировать операционную систему, в случае перерыва в работе с ПЭВМ

2.10. После 3 неудачных попыток получения доступа к ПЭВМ «Интернет-банк» учетная запись пользователя должна быть заблокирована на 30 минут или до момента разблокировки учетной записи соответствующим администратором.

2.11. Принудительно завершайте сессию работы с системой «Интернет-банк», выходом из системы.

2.12. Не храните логин и пароль в мобильном телефоне, смартфоне.

2.13. При отсутствии активности работника на ПЭВМ после авторизации, в течение 5 минут сеанс работы должен быть заблокирован или завершен.

3. Рекомендации по эксплуатации внешнего ключевого носителя

3.1. В качестве внешнего ключевого носителя для хранения ключей ЭП используется сертифицированный ФСБ USB-токен JaCarta-2 ГОСТ. Использование данного USB-токена позволяет исключить вероятность хищения ключей ЭП злоумышленниками.

3.2. Для надежной защиты ключа ЭП на USB-токене рекомендуется установить надежный пароль (PIN-код) согласно рекомендаций Раздела 2 настоящих Рекомендаций.

3.3. Список лиц, имеющих доступ к внешнему ключевому носителю, определяется приказом или распоряжением руководства Клиента, согласно закрепленными за ними функциями и полномочиями.

3.4. Порядок хранения и использования внешнего ключевого носителя с ключом ЭП должен исключать возможность несанкционированного доступа к ним.

3.5. Внешний ключевой носитель должны храниться только у тех лиц, которым они принадлежат.

3.6. Во время работы с внешним ключевым носителем доступ к ним посторонних лиц должен быть исключен.

3.7. Внешний ключевой носитель должен быть установлен в ПЭВМ с системой «Интернет-банк» только в момент подписания.

3.8. Для хранения внешнего ключевого носителя должны применяться надежные металлические сейфы.

3.9. По окончании рабочего дня, а также вне времени сеансов связи с системой «Интернет-банк» внешний ключевой носитель должен храниться в сейфе.

3.10. Хранение внешнего ключевого носителя допускается в одном сейфе с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц (произвести опечатывание упаковки).

4. Рекомендации по работе с системой “Интернет-банк».

4.1. Вход в систему «Интернет-банк» осуществляйте только с официального сайта Банка в сети Интернет по адресу:

https://www.rdb.ru/ - официальный сайт Банка;

https://corp.rdb.ru/ - Интернет-банк для юридических лиц.

Банк никогда не помещает ссылки на страницу входа в систему «Интернет-банк» в исходящей корреспонденции Клиентам.

4.2. Не входите в систему «Интернет- банк» из источников в Интернет, т.к. мошенники часто фабрикуют фишинговые сайты (сайты-двойники) для хищения Вашей аутентификационной (логин, пароль) и, как следствие, финансовой информации. При обнаружении сайта-двойника немедленно сообщите об этом в службу технической поддержки Банка и перешлите ссылку, с которой осуществлялся вход на него, для проведения расследования специалистами Банка.

4.3. При одновременном использовании нескольких ключей ЭП, следует осуществлять работу с системой «Интернет-банк» с разных ПЭВМ с хранением ключей ЭП на отдельных внешних ключевых носителях.

4.4. Рекомендуется подключить SMS-уведомление о движении денежных средств по расчетному счету.

4.5. Обязательно контролируйте движение денежных средств по выписке, предоставляемой по системе «Интернет-банк».

4.6. Рекомендуется просматривать созданные и отправленные в течение дня ЭД в системе «Интернет-банк» на предмет отсутствия несанкционированных распоряжений на перевод денежных средств (платежных поручений). В случае обнаружения таких платежей незамедлительно обратитесь в Банк.

4.7. Незамедлительно заблокируйте Вашу учетную запись, если обнаружили операции, которые Вы не совершали, успешные или неуспешные попытки входа с неизвестных Вам IPадресов или в отличное для Вас время суток.