Рекомендации по безопасному использованию системы «РК Бизнес Онлайн»

1. Используйте вход в систему «РК Бизнес Онлайн» только с официального сайта системы (**https://online.roscap.ru**) или с официального сайта Банка (https://domrfbank.ru). Ни при каких обстоятельствах не вводите логин и пароль, предназначенный для входа в систему «РК Бизнес-онлайн», на других сайтах.
2. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова и пр.) ни при каких обстоятельствах не сообщайте данную информацию.
3. Не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.
4. Используйте надежные пароли - длиной не менее 8 символов, содержащие буквы из различных регистров (заглавные и строчные), специальные символы (*, !, % и т.п.) и цифры. Не используйте очевидные сочетания (имя, фамилия, дата рождения, номер телефона). Меняйте пароли не реже одного раза в 90 дней.
5. Подключайте USB-токен к компьютеру только на время работы с системой.
6. Хранение USB-токенов должно быть организовано в месте, недоступном для посторонних лиц.
7. При любых подозрениях на компрометацию пароля посторонними лицами (в том числе представившимися сотрудниками Банка), следует незамедлительно остановить работу в системе и обратиться в Банк.
8. Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением.
9. Регулярно выполняйте антивирусную проверку на Вашем компьютере для своевременного обнаружения вредоносных программ.
10. Своевременно устанавливайте обновления операционной системы Вашего компьютера, рекомендуемые компанией-производителем.
11. Регулярно выполняйте обновления браузера, который Вы используете для работы в системе «РК Бизнес Онлайн. Данные действия значительно повысят уровень его безопасности.
12. Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент и пр.
13. Наличие прав администратора на компьютере пользователя, работающего с системой «РК Бизнес Онлайн», нежелательно.
14. Всегда корректно завершайте работу в системе в соответствии с указаниями Руководства пользователя (кнопка ).
15. Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.
16. Подключите в Банке услугу SMS-информирования о движении денежных средств на расчетном счете.
17. По возможности исключите работу в системе «РК Бизнес Онлайн» и подготовку платежных документов на общедоступном компьютере или в сетях общественного доступа (в том числе в Интернет-кафе, в зоне бесплатного Wi-Fi и пр.).
18. Исключайте посещение сайтов сомнительного содержания и любых других Интернет-ресурсов непроизводственного характера (социальные сети, конференции, чаты и т.п.) с компьютеров, на которых осуществляется подготовка и отправка документов в Банк по системе «РК Бизнес Онлайн». Также следует исключить чтение почты и открытие почтовых вложений от неизвестных источников.
19. В случае сбоев в работе компьютера или его поломки во время либо после работы с системой «РК Бизнес Онлайн» (проблемы с загрузкой операционной системы, выход из строя жесткого диска и т.п.) следует немедленно извлечь USB-токен и выключить компьютер, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.
20. Обращайте внимание на любые изменения в привычных для Вас процессах работы с системой «РК Бизнес Онлайн». При возникновении сомнений в корректности работы системы «РК Бизнес Онлайн» незамедлительно обратитесь в Банк.
21. При подтверждении операций одноразовым SMS-паролем контролируйте соответствие реквизитов операции и реквизитов в SMS-сообщении с одноразовым паролем.

22. Не пользуйтесь системой «РК Бизнес Онлайн» с того же мобильного телефона (иного устройства), на который приходят SMS-сообщения с одноразовым паролем.
23. При утрате мобильного телефона, на который Банк отправляет SMS-сообщения с одноразовым паролем, а также в случае, если у Вас неожиданно перестала работать телефонная SIM-карта, следует оперативно обратиться к своему оператору сотовой связи для блокировки абонентского номера и замены SIM-карты. Также обратитесь в Банк для выявления возможных несанкционированных операций.