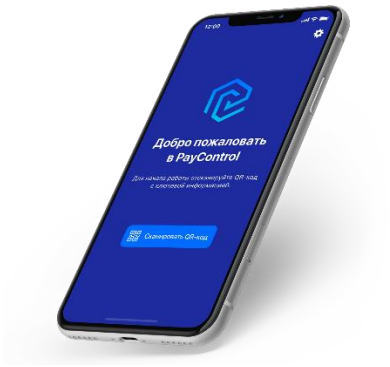
АО КБ «Урал ФД». Универсальная лицензия ЦБ РФ №249 от 09.04.2020 г.
Россия, 614066. Пермь, ул. Стахановская, 54 стр. Д. Тел. 8(342)240 10 40

Руководство по безопасности использования системы ДБО Corporate для клиентов АО КБ «Урал ФД»

Уважаемые клиенты! Для защиты от угроз Банк настоятельно рекомендует использовать следующие решения:

1. Технические меры и средства защиты.

- **PayControl –** мобильное приложение для смартфонов (iOS и Android), выполняющее функции управления ключевой информацией. Приложение хранит и защищает ключи доступа, отображает информацию по операции перед подтверждением и позволяет подтверждать операции с помощью Face ID, Touch ID или код-пароля.



- **Носители ключей (Рутокен).** Используйте защищенные устройства (Рутокен) для хранения ключей электронной подписи, которые защищают их от копирования. Подключайте носитель только на время осуществления сеанса работы в системе. Производите его извлечение из USB-порта сразу после подписания платежных поручений.

- **OTP-коды / SMS-коды.** Используйте генерацию одноразовых паролей для дополнительной авторизации. Одноразовый пароль действует только в течение одного сеанса связи.
- **Антивирусная защита.** Используйте антивирусное ПО российских производителей с регулярным обновлением антивирусных баз. Рекомендуется использовать ПО из единого реестра российского программного обеспечения. Настройте регулярную автоматическую (не реже одного раза в неделю) полную проверку устройства, с которого осуществляется доступ в систему ДБО, автоматическую проверку входящих файлов и ссылок при переходе на страницы в сети Интернет.
- **Обновление систем.** Своевременно обновляйте операционные системы и прикладное программное обеспечение в соответствии с рекомендациями производителей.
- **Мониторинг и выявление угроз.** Используйте решения для мониторинга и выявления киберугроз и оперативного реагирования на инциденты (MDR-решения).

2. **Контроль доступа и парольная политика.**

– **Ограничение мест работы.** Разместите персональный компьютер, с которого осуществляется вход в систему ДБО, в местах, исключающих несанкционированный и неконтролируемый доступ к нему посторонних лиц.

  Исключите возможность работы с системой ДБО с устройств в общественных местах, а также через публичные бесплатные Wi-Fi-сети.

  Исключите работу с недоверенными Интернет-ресурсами с устройств, с которых осуществляется доступ в систему ДБО. Маршрутизируйте трафик таким образом, чтобы разрешать соединения только с доверенными ресурсами.

  Обеспечьте работу пользователя на персональном компьютере, используемом для доступа в систему ДБО, под учетной записью с минимальными привилегиями, не допускающими установку программного обеспечения и изменения системных параметров.

– **Смена пароля.** Регулярно меняйте пароль не реже 1 раза в 90 дней.

– **Требования к паролю.** Установите пароль на устройствах, которые используются для осуществления и (или) подтверждения операций.

  Длина пароля должна быть не менее 8-ми символов для доступа к персональным компьютерам с присутствием цифр, заглавных и строчных букв, не менее 6-ти символов для доступа к мобильным устройствам.

– **Запрет передачи.** Не передавайте пароли, носители ключевой информации, СМС, OTP-коды третьим лицам.

– **Хранение средств защиты.** Храните носители ключевой информации (Рутокен) в запираемом на ключ шкафу или сейфе, доступ к которому предоставляется только уполномоченному лицу.

3. **Контроль операций и сетевая безопасность.**

– **Многоуровневый контроль.** Обеспечьте строгий контроль при формировании и подписании платежных документов, в том числе зарплатных реестров.

– **Проверка реквизитов.** Проверяйте реквизиты получателей, особенно при первом платеже, и контролируйте их изменения у контрагентов.

– **Права доступа.** Работа пользователя в системе ДБО должна осуществляться под учетной записью с минимальными правами.

– **Ограничение ПО.** Исключите возможность импорта сертификатов подписи на рабочие ПК работников бухгалтерии и финансового отдела.

– **Ограничьте установку стороннего ПО.** С помощью аппаратных или программных средств сетевой защиты (Firewall, корпоративные прокси-серверы) ограничьте доступ в сеть «Интернет». Не допускайте использование работниками организации рабочих устройств для личного использования, в том числе посещения развлекательных ресурсов, личной электронной почты или общения в мессенджерах.

4. **Безопасность электронной почты.**

- **Антиспам и Антифишинг.** По возможности используйте системы защиты с механизмом автоматического анализа ссылок и вложений.
- **Бдительность.** Не открывайте вложения от неизвестных отправителей.

  Проверяйте электронный адрес отправителя даже при внешнем сходстве с адресом контрагента.

  Не переходите по ссылкам из сомнительных писем.

  Проверяйте корректность введенного адреса для доступа в систему ДБО во избежание ввода своих учетных данных на фишинговых страницах. Корректный адрес системы ДБО https://dbo.uralfd.ru/.

5. **Обучение работников.**

- **Регулярность.** Проводите инструктаж работников по правилам информационной безопасности при приеме на работу и регулярно (не реже одного раза в год).
- **Тематика.** Обучайте работников выявлению мошеннических схем и информируйте их о новых способах атак, обучайте противодействию социальной инженерии и фишингу.
- **Регламент.** Закрепите порядок действий при подозрении на мошенничество.

Что делать при выявлении несанкционированного доступа к системе*?

1. Не перезагружайте компьютер, не запускайте антивирусные решения;
2. Извлеките токены доступа и съемные носители информации;
3. Отключите устройство от локальной сети и сети «Интернет»;
4. Выполните процедуры создания образов оперативной памяти и жесткого диска с использованием специализированного программного обеспечения (например, FTK Imager**) для дальнейшего проведения расследования;
5. Сохраните образец вредоносного программного обеспечения для проведения анализа и последующей передачи его в Банк (в рамках анализа компьютерного инцидента);
6. В случае заражения мобильного устройства, включите авиа-режим и извлеките SIM-карту.

   Если в устройстве используется электронная сим-карта, допустимо выключить устройство.

   Сбрасывать устройство до заводских настроек не рекомендуется, так как это приведет к удалению следов вредоносной активности и затруднит дальнейшее проведение расследования.

*__К несанкционированному доступу к вашему устройству и к системе ДБО__ относятся: обращения к сервисам системы ДБО в нетипичные (нехарактерные) промежутки времени, обнаружения не санкционированно установленных средств удаленного доступа (например, AnyDesk), динамическое обновление структуры, стиля или контента веб-страницы, многократное использование данных из буфера обмена (использование функции вставки), изменение параметров видеокарты оконечного устройства (использование виртуализации видеодрайвера), выявление аномалий в движение курсора мыши при работе с системой ДБО, являющихся признаком работы скриптов, роботизированных сценариев использования системы (неестественная траектория курсора, скорость перемещения курсора, скорость нажатия на кнопки мыши и время паузы, а также движение курсора при заблокированном экране), постоянное «зависание» компьютеров, которые используются для доступа к системе ДБО.
**__FTK Imager__ — бесплатный инструмент для создания криминалистических образов цифровых носителей и первоначального анализа данных, разработанный компанией AccessData (в 2020 году вошла в состав Exterro). Программа широко применяется специалистами по цифровой криминалистике для сбора, фиксации и предварительного исследования цифровых доказательств без изменения исходной информации.

При утере устройства, на которое поступают СМС-коды подтверждения и (или) установлено мобильное приложение PayControl, а также при утере Рутокена, выявлении любой подозрительной активности незамедлительно обращайтесь в Банк по телефону 8 800 100 10 40.