УТВЕРЖДАЮ
Директор
_____ К.В.Багмет
Приложение №10 к приказу №26
от «29» апреля 2019 года

ПОЛИТИКА
использования систем «клиент-банк»
ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы»

1. Общие положения

Данный документ (далее – Политика) устанавливает требования и процедуры использования систем «клиент-банк».

Системы «клиент-банк» используются для удаленного управления счетами ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы» (далее – Центр ДПО), удаленного получения банковских услуг и отправки электронных платежных и текстовых документов.

Электронный платежный документ (далее ЭПД) – документ, являющийся распоряжением Центра ДПО для совершения операций по его счетам в Банке, подписанный (защищенный) электронной подписью и имеющий равную юридическую силу с платежными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

К ЭПД относятся:

1) платежные поручения;
2) заявление на перевод иностранной валюты;
3) поручение на покупку иностранной валюты;
4) заявка на продажу валюты;
5) поручение на конвертацию иностранной валюты;
6) поручение на проведение операций по транзитному счету.

ЭПД создается Центром ДПО на основе бумажного документа либо на основании другого электронного документа и полностью повторяет его по содержанию.

Электронный текстовой документ (далее ЭТД) – документ, подписанный (защищенный) электронной подписью и обеспечивающий обмен информацией при совершении расчетов по счетам Клиента (реестры, выписки, счета за ведение электронного документооборота и обслуживание системы «клиент-банк», служебная информация).

Пользователь системы «клиент-банк» – работник Центра ДПО, на имя которого Банком выданы криптографические ключи, позволяющие

подписывать и направлять электронные документы.

Установку, управление средствами защиты информации системы «клиент-банк» в Центре ДПО осуществляет Администратор систем «клиент-банк».

2. Меры защиты системы «клиент-банк»

Информационная безопасность при работе с системой «клиент-банк» обеспечивается следующими мерами защиты:

1) Идентификацией и аутентификацией пользователей с использованием механизмов системы «клиент-банк»;
2) Разделением ролей пользователей так, чтобы исключить возможность бесконтрольного пользования банковскими услугами одним работником;
3) Применением электронной подписи, которая позволяет обеспечить целостности и аутентичности (доказательство авторства) электронных документов;
4) Хранением ключа электронной подписи на защищенном съемном носителе информации (eToken);
5) Применением средств криптографической защиты информации при передаче её между Центром ДПО и Банком;
6) Выделением автоматизированного рабочего места, используемого только для работы с системами «клиент-банк» (далее – АРМ СКБ), на котором запрещено выполнение другой деятельности работника.

Информационная безопасность АРМ СКБ обеспечивается также общими мерами защиты в рамках СИБ Центра ДПО, такими как:

1) управление доступом к операционной системе;
2) антивирусная защита;
3) защита межсетевого взаимодействия;
4) ограничение доступа в помещение с АРМ СКБ;
5) резервное копирование и восстановление информации и т.п.

Как правило, в части системы «клиент-банк», размещенной на стороне Банка применяются меры по выявлению мошеннических операций.

3. Роли пользователей системы «клиент-банк»

В Центре ДПО разграничение прав пользователей системы «клиент-банк» основано на применении ролей. Роль – это условное обозначение всей совокупности прав и возможностей каждого конкретного пользователя по работе в системе. Роли задают возможность и уровень доступа к определённым данным СКБ и возможность выполнения определённых операций.

В системы «клиент-банк» используются следующие роли:

Название роли	Задача роли
Контроллер	Контроль за проводимыми Оператором

Название роли	Задача роли
	системы финансовыми операциями
Оператор системы	Осуществление финансовых операций через систему «клиент-банк»

4. Обязанности пользователей системы «клиент-банк»

Доступ к использованию системы «клиент-банк» и носителям ключа электронной подписи необходимый для выполнения служебных обязанностей, предоставляется работнику Центра ДПО в соответствии с «Политикой управления доступом к информационным ресурсам».

Пользователи системы «клиент-банк» обязаны:

1) осуществлять работу в системе «клиент-банк» только от имени своей учетной записи;

2) использовать только тот ключ электронной подписи, доступ к которому получен официально в соответствии с «Политикой управления доступом к информационным ресурсам»;

3) незамедлительно уведомлять о случаях возникновения сбоев и некорректного завершения бизнес-значимых операций в системе «клиент-банк»;

4) при работе в системе «клиент-банк» подключаться к банку, только на время приема/передачи электронных документов, в остальное время сеанс связи должен быть отключен, а носитель ключа электронной подписи необходимо хранить в сейфе;

5) осуществлять регулярный контроль состояния счетов и незамедлительно информировать администратора системы «клиент-банк», работника, ответственного за экономическую безопасность и службу технической поддержки Банка обо всех подозрительных или несанкционированных операциях;

6) незамедлительно информировать службу поддержки Банка при наличии проблемы с подключением;

7) осуществлять контроль за корректностью и актуальностью вводимых данных в систему «клиент-банк»;

8) осуществлять контроль за выгруженными документами для получения/передачи во внешние системы;

9) в случае выхода из строя АРМ СКБ, либо сбое на нем программного обеспечения: завершить работу на АРМ СКБ, выключить его и извлечь носитель ключа электронной подписи;

10) в случае утери носитель ключа электронной подписи или подозрении на несанкционированный доступ к ключу электронной подписи уведомить работника, ответственного за экономическую безопасность и Банк.

Пользователю системы «клиент-банк» запрещается:

1) передавать другому работнику ключ электронной подписи или свои учетные данные для доступа в систему «клиент-банк»;

2) использовать ключ электронной подписи или учетные данные другого работника для доступа в систему «клиент-банк»;

3) хранить ключи электронной подписи на жестких дисках АРМ СКБ;

4) оставлять носители ключа электронной подписи подключенными к АРМ СКБ в свое отсутствие на рабочем месте;

5) использовать на АРМ СКБ другие сервисы или системы, не связанные с системой «клиент-банк»;

6) сообщать в устной или письменной форме информацию системе «клиент-банк» (пароли, кодовые слова, и пр.) кому-либо по телефону, электронной почте или через другие средства связи.

5. Обязанности администратора системы «клиент-банк»

В обязанности администратора системы «клиент-банк», входит:

1) после согласования заявки на предоставления доступа к системе «клиент-банк», обеспечить подключение пользователя к системе «клиент-банк», согласно подписанной заявке, в срок не более двух дней;

2) обеспечение информационной безопасности системы «клиент-банк»;

3) обеспечение непрерывности работы и восстановление в случае прерываний для компонентов системы «клиент-банк» расположенных в Центре ДПО;

4) обеспечение резервного копирования ПО и конфигурации системы «клиент-банк»;

5) проведение оценки совместимости ПО системы «клиент-банк» с существующим ПО при покупке программного обеспечения стороннего разработчика.

При получении информации о подозрительных или несанкционированных операциях, потере носителей или компрометации ключей электронной подписи администратор системы «клиент-банк» совместно с СЭБ:

1) проводят расследование инцидентов;

2) уведомляют и взаимодействуют со службой поддержки Банка;

3) уведомляют и привлекают правоохранительные органы в случае необходимости.