УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

РЕГЛАМЕНТ
ИСПОЛЬЗОВАНИЯ СИСТЕМЫ КЛИЕНТ-БАНК

2018 г.

Оглавление

1. Общие положения

1.1. Настоящие правила вводятся в целях обеспечения соблюдения политики в сфере информационной безопасности, а также с целью предотвращения ненадлежащего использования компьютерного оборудования.

1.2. Настоящие правила устанавливают общие принципы, условия и порядок электронного документооборота с обслуживающими ООО «Сатурн» (далее – Компания) банками, осуществляемого с помощью системы «Клиент-Банк» (далее - СКБ).

1.3. Настоящие правила определяют права и обязанности пользователей СКБ, специалистов отдела информационных технологий (ИТ/ИБ), обеспечивающих мероприятия по обеспечению информационной безопасности.

2. Описание программно-аппаратного комплекса СКБ

2.1. СКБ является информационной системой, организованной Банком и обеспечивающей взаимодействие Банка и клиента – Компании – с использованием технических средств в целях обеспечения электронного документооборота.

2.2. На стороне Компании СКБ содержит следующие компоненты:

- Клиентское программное обеспечение СКБ обслуживающего Банка, включая средства криптозащиты информации (СКЗИ). Допускается установка СКБ разных обслуживающих банков в рамках единого рабочего места.
- Системное программное обеспечение – операционная система, средства ограничения несанкционированного удаленного и/или непосредственного доступа к рабочему месту.
- Выделенный персональный компьютер с аппаратно-программными средствами защиты от несанкционированного доступа, изолированный от ресурсов корпоративной компьютерной сети Компании, подключенный к централизованному узлу доступа в сеть Интернет – рабочее место.
- Защищенная сеть передачи данных.
- Узел централизованного доступа в сеть Интернет.

2.3. Информационный обмен в рамках СКБ осуществляется по открытым каналам связи с использованием электронного документооборота по сети Интернет.

2.4. Электронный документооборот включает в себя процесс формирования

электронного документа (далее - ЭД), подписание его электронно-цифровой подписью (далее - ЭЦП) и/или цифровой подписью (далее - ЦП), передачу ЭД получателю, проверку ЭД на подлинность (проверка ЭЦП), а также учет и хранение ЭД.

2.5. В целях обеспечения электронного документооборота Банк осуществляет управление сертификатами ключей ЭЦП.

2.6. Носители с ключами должны храниться в специально отведенном месте (сейфе) и устанавливаются в компьютер только на время работы с программой.

2.7. Рабочее место СКБ должно быть снабжено парольным входом в компьютер. При необходимости перерыва в работе оператор должен выйти из программы и осуществить блокировку клавиатуры и экрана ПК средствами установленной системы защиты от несанкционированного доступа. После завершения работы выключить ПК, носители с ключами убрать в место хранения.

2.8. В случае отсутствия владельца ЭЦП (отпуск, болезнь и т.д.) к обработке электронных документов с ЭЦП допускается ответственное лицо, назначенное Приказом по Компании.

2.9. Плановая смена рабочих ключей происходит по согласованию с Банком.

2.10. Ключевые носители с секретными ключами ЭЦП и шифрования (секретными ключами ЦП и кодирования), а также инсталляционные носители с программным обеспечением СКЗИ необходимо взять на поэкземплярный учет в выделенных для этих целей журналах;

2.11. Рабочие комплекты ключей (и их копии) и комплекты резервных ключей хранятся раздельно с обеспечением условия невозможности их одновременной компрометации или уничтожения;

2.12. Лица ответственные за учет и хранение секретных ключей назначаются приказом по Компании.

3. Порядок использования СКБ

3.1. Взаимодействие корпоративной информационной системы и СКБ

Подготовка платежного документа выполняется средствами корпоративной информационной системы Компании.

Сформированный документ сохраняется в виде выходного файла и записывается на сменный flash-носитель информации.

Сменный flash-носитель устанавливается в USB-порт рабочего места СКБ, содержащиеся на нем сформированные документы загружаются пользователем в клиентское программное обеспечение СКБ для последующего формирования электронных платежных документов.

Полученные из банка электронные документы аналогичным способом переносятся пользователем в корпоративную информационную систему, где ведется архив отправленных и полученных документов.

3.2. Использование СКБ

Использование программного обеспечения СКБ Банка необходимо осуществлять в

соответствии с «Регламентом электронного документооборота», предоставляемым Банком.

3.3. Ситуации компрометации ключевой информации

Понятие компрометации означает, что произошло нарушение безопасности хранения и использования ключа, в результате которого возникла вероятность несанкционированного его применения и нанесения тем самым ущерба Компании. К событиям, связанным с компрометацией ключей относятся:

- Утрата носителя (оригинал и/или дубликат) с закрытыми ключами;
- Утрата носителя (оригинал и/или дубликат) с закрытыми ключами с ее последующим обнаружением;
- Утрата ключей от сейфа в момент нахождения в нем носителей ключевой информации;
- Увольнение сотрудников, имевших доступ к ключевой информации;
- Носитель с закрытыми ключами стал на время доступен постороннему лицу без контроля со стороны владельца/пользователя;
- Обнаружен случай подписания электронного документа ЭЦП кем-либо, кроме самого владельца/пользователя ЭЦП;
- Нарушение печати на сейфе (контейнере, пенале) с ключами;
- Иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к секретному ключу ЭЦП (ЦП) посторонних лиц.

При установлении факта компрометации действующих ключей должны быть приняты следующие меры:

- Поставить в известность главного бухгалтера Компании, руководителя подразделения, обеспечивающего надзор за соблюдением правил информационной безопасности в Компании, действующего на основании договора оказания услуг персоналом;
- Направить по каналу электронной связи в Банк текстовый файл с уведомлением (согласно Регламенту обслуживающего Банка) о компрометации ключей, которое подписывается скомпрометированной ЭЦП. При наличии резервных ключей, в уведомление необходимо добавить оповещение о переходе на использование резервных ключей;
- Немедленно прекращается обмен информацией с использованием скомпрометированных ключей. Формируется запрос на получение нового комплекта рабочих ключей;
- До получения новых рабочих ключей, для обмена данными с Банком применять резервные ключи, либо перейти на бумажный документооборот.

Выход из строя носителя с закрытыми ключами не рассматривается как компрометация ключей.

4. Права и обязанности пользователей СКБ

4.1. Пользователи СКБ

Пользователями СКБ являются сотрудники Компании, выполняющие действия по проведению электронных платежей с ЭЦП в СКБ.

Список пользователей СКБ и возложение на них обязанности исполнения требований настоящих Правил в целях обеспечения информационной безопасности утверждается Приказом по Компании.

4.2. Пользователи обязаны:

Осуществлять платежи с использованием СКБ в соответствии с утвержденным действующим финансовым планом (включая изменения и приложения к плану), а также при наличии первичных акцептованных документов в порядке очередности, указанной непосредственным руководителем.

Использовать клиентское программное обеспечение СКБ в соответствии с «Регламентом электронного документооборота», предоставляемым Банком.

В целях проведения электронных платежей с ЭЦП получить у представителя Банка два носителя (оригинал и копия) ключей для электронно-цифровой подписи, а также резервные ключи.

В технологическом процессе использовать копию ключей, а в случае выхода ее из строя (механическое повреждение и т.д.) – оригинал, до создания новой копии ключа.

Хранить ключи в опечатанном владельцем ЭЦП сейфе (контейнере, пенале). При хранении рабочих ключей в одном сейфе (металлическом шкафу) с другими документами они помещаются в отдельный опечатываемый контейнер. Условия хранения носителей с ключами должны исключать возможность коробления, изгиба под воздействием температуры или другим причинам, а также воздействия пыли, магнитных и электрических полей.

Обеспечить сохранность ключей ЭЦП и шифрования (ЦП и кодирования), паролей для входа в СКБ и другой конфиденциальной информации от несанкционированного доступа.

В целях обеспечения информационной безопасности пользователь обязуется соблюдать «Рекомендации клиенту СКБ по обеспечению безопасности информации при эксплуатации» - Приложение к договору об использовании СКБ Банка.

Своевременно доводить до сведения специалистов отдела ИТ/ИБ информацию об изменениях правил или режима работы СКБ, инициированных Банком, а также сроки и порядок вступления в силу этих изменений (не позднее, чем за десять рабочих дней до даты вступления в силу данных изменений и дополнений).

4.3. Пользователям запрещается:

- Выводить на монитор, печатающее устройство ключевую информацию (ключи);
- Самостоятельно изготавливать копии ключей;
- Передавать кому-либо носитель с ключами, flash-носитель с данными;
- Оставлять компьютер СКБ и носители с ключами без принятия мер по защите их от несанкционированного доступа.

4.4. Пользователи имеют право:

- Получать консультацию у специалистов отдела ИТ/ИБ, по работе с компьютерным оборудованием и программным обеспечением, по вопросам компьютерной безопасности;

- Вносить предложения по изменению настоящих правил;
- Получать уведомления об изменениях настоящих правил и правил работы на конкретном оборудовании.

5. Права и обязанности специалистов отдела ИТ/ИБ

5.1. Специалисты отдела ИТ/ИБ обеспечивают исправность оборудования и системного программного обеспечения СКБ, обеспечивают выполнение всех необходимых технических мероприятий для функционирования программного обеспечения клиентской части СКБ.

5.2. Ответственность за исправное функционирование оборудования и системного программного обеспечения СКБ, за соблюдение технических требований информационной безопасности в целях настоящих Правил возлагается на сотрудников отдела ИТ/ИБ.

5.3. Специалисты отдела ИТ/ИБ обязаны:

- Проверять исправность оборудования рабочего места СКБ, правильность функционирования программного обеспечения и соблюдение правил работы, с использованием, при необходимости, административного доступа на время проверки;
- По согласованию с главным бухгалтером Компании оперативно отключать компьютер СКБ от защищенной сети передачи данных, блокировать работу или выводить из эксплуатации оборудование в случае нарушения информационной безопасности, по причине неисправности оборудования или грубого нарушения Правил пользователями СКБ;
- Предоставлять пользователям СКБ информацию необходимую для работы на компьютерном оборудовании;
- Доводить до сведения пользователей СКБ информацию об изменении правил или режима работы СКБ, инициированных специалистами ИТ/ИБ по техническим причинам;
- Снижать до минимально необходимого время простоя оборудования вследствие неполадок или сервисных работ;
- Создавать копии рабочих ключевых носителей с секретными ключами ЭЦП и шифрования, которые будут использоваться в работе с СКБ в присутствии лица, ответственного за данную ЭЦП;
- Не разглашать информацию, полученную в ходе выполнения служебных обязанностей;

5.4. Специалисты отдела ИТ/ИБ имеют право:

- Проводить проверки содержимого компьютера СКБ на предмет его профильного использования;
- Делать предупреждения пользователям СКБ, нарушившим настоящие Правила;
- Доводить до сведения руководства пользователей СКБ факты грубого или неоднократно нарушения настоящих Правил;
- Требовать от пользователя СКБ подробного отчета о работе, если во время этой

работы произошел отказ или сбой оборудования, или программного обеспечения;

- Без предупреждения удалять с дисков СКБ файлы пользователей, содержащие игровые программы и программы, предназначенные для нарушения компьютерной безопасности, файлы, зараженные компьютерными вирусами, файлы, содержащие мультимедиа информацию, не имеющую отношения к профилю деятельности Компании с доведением до сведения своего непосредственного руководителя.