

# ***ООО МКК «Центр Займов г.Киров»***

610002, Россия, г. Киров, ул. Ленина, 102-а, , тел./факс (8332) 410-414,  
E-mail:centrzaimovkirov@gmail.com

«УТВЕРЖДАЮ»:

Директор ООО МКК «Центр Займов г. Киров»

Демин С.П.

(подпись)

« 31 » мая 2019г.

## **ПОРЯДОК**

**ЗАЩИТЫ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ  
ФИНАНСОВЫМ ОПЕРАЦИЯМ**

**«ООО МКК ЦЕНТР ЗАЙМОВ Г. КИРОВ»**

## **СОДЕРЖАНИЕ**

- 1. Общие положения**
- 2. Термины и определения**
- 3. Риски использования защищаемой информации для совершения незаконных финансовых операций**
- 4. Меры по защите информации**
  - 4.1. ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ**
  - 4.2. ЗАЩИТА ЭЛЕКТРОННЫХ СРЕДСТВ ДОСТУПА И ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ (ЭСДДО) ОТ КОМПРОМЕТАЦИИ**
  - 4.3. ЗАЩИТА ХРАНЯЩЕЙСЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ИСПОЛЬЗОВАНИЯ**
  - 4.4. ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ**
  - 4.5. МЕРЫ ОРГАНИЗАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ СВОИХ КЛИЕНТОВ**

### **Приложения:**

**Приложение 1.** Журнала учета пользователей защищаемой информации

**Приложение 2.** Рекомендации по защите информации клиента от рисков ее использования в незаконных финансовых операциях

## 1. Общие положения

1.1. Настоящий Порядок защиты информации в целях противодействия незаконным финансовым операциям (далее – Порядок) утверждается директором (далее – руководитель), пересматривается по мере необходимости в целях повышения эффективности деятельности по защите информации и является внутренним нормативным документом ООО МКК «Центр Займов г. Киров» (далее – организация), в соответствии с которым сотрудники организации при осуществлении деятельности на финансовом рынке противодействуют незаконным финансовым операциям.

1.2. Порядок разработан в соответствии с Положением Банка России от 17.04.2019 № 684-П "Положение об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций", Федеральным законом от 26.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации» и иными правовыми актами, Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи";

1.3. Деятельность организации и ее сотрудников по исполнению требований Федерального закона от 27.07.2006 N152-ФЗ "О персональных данных" настоящим Порядком не регулируется.

## 2. Термины и определения

**Деятельность в сфере финансовых рынков** – процесс принятия на обслуживание и обслуживание организацией получателей финансовых услуг в соответствии с договорами предоставления, получения займа, передачи личных сбережений, уступки денежного требования, поручительства, залога и иными договорами об оказании финансовых услуг;

**Незаконная финансовая операция** – незаконное использование денежных средств, нанесение иного убытка организации и(или) ее клиенту;

**Защищаемая информация** – информация, которая может быть использована для совершения незаконных финансовых операций, в том числе:

-электронные подписи, пароли, коды, кодовые(ключевые) слова, ключевая информация средств криптографической защиты информации (далее-СКЗИ), иная подобная информация и ее документальные и электронные носители, в совокупности являющиеся электронными средствами доступа и дистанционного обслуживания(ЭСДДО), используемые организацией и ее клиентами для авторизации(проверки прав), аутентификации(проверки подлинности), осуществления доступа в автоматизированные системы, создания электронных документов и осуществления финансовых операций;

-хранящиеся и обрабатываемые в автоматизированных компьютерных системах конфиденциальные данные, финансовые и иные сведения о деятельности организации и ее клиентов;

-находящиеся в процессе передачи по телекоммуникационным каналам документы, сообщения, пароли, коды и иная защищаемая информация;

**Защита информации** – предусмотренные настоящим Порядком меры противодействия незаконному доступу и использованию защищаемой информации;

**Автоматизированная система** – автономное устройство или комплекс(сеть) программно-технических средств и информационных технологий, позволяющих организации получать, подготавливать, обрабатывать, передавать, хранить и использовать защищаемую информацию;

**Клиент** – лицо, обратившееся в организацию за финансовой услугой либо находящееся на обслуживании в организации в соответствии с договором об оказании финансовой услуги;

### **3.Риски использования защищаемой информации для совершения незаконных финансовых операций**

1)Утрата и(или) несанкционированное использование электронных средств доступа и дистанционного обслуживания организации и ее клиентов(**компрометация ЭСДДО**);

2)Проникновение в автоматизированные системы организации и ее клиентов с использованием вредоносных кодов, программ и(или) иными способами с целью хищения, уничтожения, изменения, блокирования доступа и иного незаконного использования электронных документов, сообщений, учетных записей, иной защищаемой информации(**несанкционированный доступ**);

3)Перехват передаваемых организацией и(или) ее клиентами по телекоммуникационным каналам электронных документов и иных сообщений, в том числе электронной почты, СМС и т.д., при осуществлении ими дистанционного обслуживания и иных операций с целью их изменения, подмены, уничтожения и иного незаконного использования(**перехват сообщений**)..

## **4.Меры по защите информации**

### **4.1. ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ**

#### **4.1.1. Обязанности руководителя:**

-разработка, изменение и утверждение внутренних регулирующих актов, определение мер в сфере защиты информации в соответствии с требованиями законодательства и обстоятельствами;

-организация деятельности сотрудников по исполнению регулирующих актов и принятых мер по защите информации, в том числе:

обеспечение должного финансирования мероприятий по защите информации и контроля за их исполнением;

организация инструктажей для сотрудников-пользователей защищаемой информации;

определение видов используемой организацией ЭСДДО, другой защищаемой информации;

установление полномочий, обязанностей и ответственности пользователей защищаемой информации;

контроль за ведением и хранением Журнала учета пользователей защищаемой информации(Приложение 1);

принятие мер по защите информации клиентов, в том числе размещение в местах оказания услуг Рекомендаций по защите информации клиента от рисков ее использования в незаконных финансовых операциях(Приложение 2)

- в случае увольнения сотрудника проведение с ним окончательного расчета только после принятия руководителем или уполномоченным им лицом всей защищаемой информации, пользователем которой он был;
- ограничение доступа к носителям защищаемой информации;
- иные меры по соблюдению конфиденциальности защищаемой информации

#### **4.1.2.Обязанности системного администратора:**

- участие в разработке внутренних регулирующих актов организации в сфере защиты информации и определении мер организации, направленных на защиту информации;
- согласование принимаемых им мер по защите информации с руководителем;
- контроль за надлежащим функционированием и использованием применяемых организацией аппаратных, программных и иных средств защиты информации;
- выявление фактов и обстоятельств компрометации ЭСДДО, других событий, связанных с нарушением защиты информации, немедленное информирование руководителя о таких событиях, принятие мер по минимизации негативных последствий и их предотвращению в будущем;
- ведение Журнала учета пользователей защищаемой информации(Приложение 1);
- проведение инструктажей с пользователями защищаемой информации;
- контроль за загрузкой пользователями в автоматизированные системы программного обеспечения;
- иные обязанности по соблюдению конфиденциальности и защите информации в соответствии с распоряжениями руководителя;

#### **4.1.3.Пользователями защищаемой информации в организации являются:**

- Руководитель
- Бухгалтер
- Системный администратор, иной специалист по информационным технологиям
- Юрист(ответственный сотрудник по ПОД/ФТ/ФРОМУ)
- Менеджеры по работе с клиентами

### **4.2.ЗАЩИТА ЭЛЕКТРОННЫХ СРЕДСТВ ДОСТУПА И ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ (ЭСДДО) ОТ КОМПРОМЕТАЦИИ**

#### **4.2.1.Используемые организацией ЭСДДО**

- пароль доступа, электронная подпись и ее носитель для взаимодействия с ФНС, ФСС, ПФ, Федеральной службой государственной статистики и другими государственными органами
- пароль доступа, электронная подпись и ее носитель для предоставления и обмена электронными сообщениями через личные кабинеты организации на сайте Росфинмониторинга и Банка России;
- пароль доступа, электронная подпись и ее носитель для работы организации в Личном кабинете на сайте бюро кредитных историй
- пароль доступа, электронная подпись и ее носитель для дистанционного банковского обслуживания(ДБО);
- иные электронные подписи и их носители;
- программа криптографической защиты информации КриптоПро CSP и ее носитель;
- иные программы криптографической защиты и их носители(программы российского производства должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности);
- пароли доступа к хранящейся в автоматизированных системах организации информации и их письменные и(или) электронные носители;

- ПИН-коды(в случае использования организацией корпоративных банковских карт), банковские карты;
- пароли доступа и СМС-коды(в случае их использования для дистанционного банковского обслуживания, для операций клиента в Личном кабинете клиента на сайте организации или иной системы дистанционного обслуживания клиента);
- пароль администратора и пользователей сайта организации

#### **4.2.2.Обязанности и ответственность пользователей ЭСДДО**

1)Пользователь ЭСДДО обязан:

- использовать ЭСДДО только в соответствии с установленными для данного пользователя правами и обязанностями;
- немедленно уведомлять руководителя обо всех случаях утраты ЭСДДО
- не предоставлять относящуюся к ЭСДДО информацию третьим лицам;
- не копировать ЭСДДО без распоряжения руководителя;
- немедленно сообщать руководителю о ставших ему известными попытках несанкционированного получения или использования ЭСДДО третьими лицами и иных связанных с защищаемой информацией инцидентах;
- не допускать несанкционированное изменение относящейся к ЭСДДО информации;
- при увольнении или отстранении от обязанностей, связанных с использованием ЭСДДО, сдать их в организацию руководителю или уполномоченному им сотруднику;
- в случае самостоятельного изменения пароля доступа или иного ЭСДДО немедленно уведомить об этом системного администратора для регистрации нового пароля в Журнала учета пользователей защищаемой информации (Приложение 1);

2)В случае неисполнения или ненадлежащего своих обязанностей по пользователь ЭСДДО несет ответственность в соответствии с законодательством и внутренними актами организации

#### **4.2.3.Компрометация ЭСДДО возникает в случае установленного факта или возникшего обоснованного подозрения о наступлении любого из следующих событий:**

- использование относящейся к ЭСДДО информации для совершения незаконной финансовой операции со средствами организации или клиента;
- несанкционированное получения относящейся к ЭСДДО информации третьими лицами;
- несанкционированный доступ в автоматизированную систему организации с использованием ЭСДДО организации третьими лицами;
- несанкционированный доступ в места закрытого хранения(сейфы, помещения и т.д.) относящихся к ЭСДДО носителей информации;
- утрата документов или устройств (флэшки, компьютера, мобильного телефона), которые были носителями электронной подписи, криптографического ключа , программы и(или) иной относящейся к ЭСДДО информации;
- несанкционированное получение защищаемой информации о финансовых операциях организации и ее клиентов третьими лицами;
- проблемное увольнение сотрудника, бывшего пользователем или имевшего доступ к ЭСДДО;

#### **4.2.4.Меры по предотвращению компрометации ЭСДДО**

- передача сотруднику относящейся к ЭСДДО информации и ее носителей только после проведения инструктажа под личную подпись в Журнала учета пользователей защищаемой информации (Приложение 1);
- установка паролей доступа(при наличии технической возможности) к устройствам, являющимся носителям относящейся к ЭСДДО информации;

-копирование относящейся к ЭСДДО информации на защищенные от несанкционированного доступа носители, находящиеся в распоряжении руководителя или уполномоченного им лица;

-установление ответственности сотрудников-пользователей ЭСДДО за компрометацию ЭСДДО по вине сотрудника в соответствии с должностной инструкцией работника(при наличии), договором с сотрудником или приказом руководителя в соответствии с тяжестью последствий наступившего в сфере защиты информации инцидента;

#### **4.2.5.Меры в случае компрометации ЭСДДО**

-в случае компрометации ЭСДДО, выданных удостоверяющим центром, банком, иной организацией, необходимо немедленно отозвать(аннулировать) ЭСДДО у лица-производителя электронного средства в соответствии с установленной им процедурой;

- в случае компрометации ЭСДДО, выданных сотрудниками организации и используемых для работы в автоматизированных системах (пользовательских паролей и кодов доступа) необходимо изменить пароли доступа и провести ревизию защищаемой информации;

-в случае компрометации используемых для обслуживания клиентов ЭСДДО, произведенных самой организацией (Личного кабинета клиента на сайте организации, системы генерации SMS-сообщений с кодом подтверждения и т.д.) необходимо немедленно отключить соответствующий сервис, уведомить об этом клиентов и принять необходимые меры для восстановления работоспособности сервиса и усиления его защищенности;

- в случае компрометации ЭСДДО, произведенного самим клиентом(пароль, код доступа в Личный кабинет, другое) необходимо немедленно прекратить оказание клиенту дистанционных услуг с использованием ЭСДДО и уведомить его об этом;

- во всех случаях необходимо провести тщательное расследование последствий, причин и обстоятельств компрометации, разработать и реализовать дополнительные меры по защите ЭСДДО

### **4.3.ЗАЩИТА ХРАНЯЩЕЙСЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ИСПОЛЬЗОВАНИЯ**

#### **4.3.1.Используемые организацией автоматизированные системы хранения информации**

- 1)Персональный компьютер
- 2)Компьютерная сеть
- 3)Система резервного копирования информации
- 4)Иные аппаратные средства
- 5)Официальный сайт организации
- 6)Базовая операционная программа
- 7)Программа криптографической защиты информации КриптоПро CSP
- 8)Базовая/отраслевая версия бухгалтерской программы (1С Предприятие 8.3)
- 9)Отраслевая учетная программа «1С Управление МФО и УПК Проф»
- 10)Иные программные средства

#### **4.3.2.Виды защищаемой в автоматизированных системах информации**

-информация о деятельности организации и ее клиентов, предоставляемая в соответствии с законодательством в государственные органы, фонды, бюро кредитных историй в виде электронных документов(отчетов) и иных сообщений, а также получаемые от них электронные документы и иные сообщения;

- хранящиеся в организации сведения и документы о клиентах, полученные в процессе исполнения организацией требований антилегализационного, отраслевого и иного законодательства, в том числе персональные данные;
- электронные подписи, криптографические программы, пароли, коды и иная относящаяся к ЭСДДО информация в случае ее хранения и обработки в автоматизированных системах;
- сведения об обязательствах и финансовых операциях, иные конфиденциальные сведения об организации и ее клиентах, хранящиеся и обрабатываемые в специализированных учетных программах и в отдельных папках и файлах;
- электронные документы и иные сообщения, возникшие в процессе обслуживания организации и ее клиентов в коммерческом банке;
- сведения об операциях клиентов и организации, получаемы и хранящиеся с использованием официального сайта организации;

#### **4.3.3.Основные угрозы и уязвимости для хранящейся в автоматизированных системах информации**

- вредоносные коды, программное обеспечение, полученные по электронной почте и из других источников;
- ссылки на потенциально опасные ресурсы;
- загрузки программ с опасных сайтов;
- неспособность антивирусных программ обезвредить все потенциально опасные атаки;
- ошибочные действия сотрудников;

#### **4.3.4.Обязанности и ответственность пользователей хранящейся в автоматизированных системах информации**

1)Пользователь обязан:

- не раскрывать полученных по электронной почте провоцирующих сообщений и ссылок, не скачивать программное обеспечение с сомнительных сайтов;
  - не изменять условия доступа к информации без согласования с руководителем или уполномоченным им лицом;
  - не копировать, не распространять, не предоставлять третьим лицам, не уничтожать без разрешения руководителя, не использовать иными способами защищаемую информацию, пользователем которой он является, либо иную конфиденциальную информацию организации, ставшую ему доступной;
  - использовать защищаемую информацию и устройства для ее хранения и обработки только в целях исполнения своих профессиональных и должностных обязанностей в интересах организации;
  - немедленно уведомлять руководителя о случаях несанкционированного доступа, прекращения доступа, утраты, использования третьими лицами, нарушения целостности информации и иных событиях с защищаемой информацией;
  - при увольнении или отстранении от обязанностей, связанных с доступом к защищаемой информации, предоставить эту информацию, ее носители руководителю или уполномоченному им сотруднику в надлежащем виде и качестве;
- 2)В случае неисполнения или ненадлежащего своих обязанностей по защите информации пользователь этой информации несет ответственность в соответствии с законодательством и внутренними актами организации

#### **4.3.5.Технические меры защиты информации в автоматизированных системах**

1.Установка и регулярное обновление операционной системы, антивирусных программ и файрволов, иных систем защиты информации от несанкционированного доступа, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;



2) Меры по управлению доступом и полномочиями, в том числе:

2.1. Установка и регулярное обновление каждому пользователю защищаемой информации персональных идентификаторов, определяющих объем его прав при работе с информацией (паролей: доступа), в том числе:

- пароля системного администратора

- пароля доступа пользователя ко всей хранящейся в персональном компьютере информации в случае использования компьютера одним пользователем;

- паролей для отдельных пользователей в случае использования компьютера разными пользователями, в том числе паролей доступа к отдельным папкам информационной базы;

- паролей доступа к отдельным папкам при размещении информации в сетевом хранилище

- паролей доступа администратора сайта и пользователей к информации на официальном сайте организации

2.2. Сигнализация, отключение доступа, задержка работ, отказ в запросе при попытках несанкционированного доступа;

3) Протоколирование и аудит (сбор, накопление и анализ) информации о событиях, происходящих в автоматизированных системах;

4) Резервное копирование, архивирование защищаемой информации, в том числе ЭСДДО, компьютерных программ, сайта, на мобильные носители и стационарные автоматизированные устройства копирования и хранения информации с высоким уровнем защиты;

5) Шифрование наиболее важной информации при хранении и передаче данных;

6) Выделение каждому постоянно занятому работой с защищаемой информацией сотруднику отдельного персонального компьютера;

#### **4.4. ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ**

**4.4.1. Виды электронных документов и иных сообщений, в отношении которых существует риск их перехвата в процессе передачи или получения организацией по телекоммуникационным каналам связи**

- предоставляемые организацией через Internet в Банк России, Росфинмониторинг, Федеральную налоговую службу, Федеральную службу государственной статистики, Пенсионный фонд РФ, Фонды социального страхования, в коммерческий банк, Бюро кредитных историй, а также получаемые от них электронные документы и сообщения;

- передаваемые через Internet или телефонную связь клиентами в организацию и от организации клиентам сообщения, в том числе электронные документы, содержащие конфиденциальную финансовую и иную информацию;

-- SMS-сообщения при использовании организацией дистанционного банковского обслуживания (ДБО);

- SMS-сообщения с кодами доступа и или подтверждения операции, иной удостоверяющей права клиента информацией в случае дистанционного обслуживания клиента с использованием сайта или иных телекоммуникационных технологий;

**4.4.2. Технические меры организации по защите передаваемых электронных сообщений**

- в случае использования организацией электронного документооборота с государственными органами, коммерческими банками и иными организациями использовать при направлении и получении электронных сообщений установленные этими организациями средства криптографической защиты информации;

- в случае использования организацией и ее клиентом электронной почты для передачи электронных документов и иных содержащих важную финансовую информацию сообщений применять PGP-ключ, обеспечивающий высокий уровень защищенности передаваемых сообщений между организацией и конкретным клиентом;
- в случае использования официального сайта организации для дистанционного обслуживания клиентов с применением паролей, PIN-кодов, SMS-сообщений и т.д.) в целях обеспечения максимальной безопасности используемых клиентами электронных средств доступа и дистанционного обслуживания(ЭСДДО) и предоставляемых ими электронных документов и иных сообщений применять SSL-сертификат;
- в случае использования организацией для дистанционного обслуживания клиентов телефонных каналов связи максимально ограничивать объем передаваемой информации и, при исполнении финансовых поручений клиента с использованием телефонной связи принимать дополнительные меры по идентификации клиента и подтверждению его полномочий.

#### **4.5. МЕРЫ ОРГАНИЗАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ СВОИХ КЛИЕНТОВ**

Дополнительно к уже установленным мерам по защите информации организация принимает следующие меры:

- 1) Доводит до своих клиентов Рекомендации по защите информации клиента от рисков ее использования в незаконных финансовых операциях(далее – Рекомендации - Приложение 2), в том числе от воздействия вредоносных кодов, следующими способами:
  - путем размещения Рекомендаций в местах оказания услуг организации, в том числе на ее официальном сайте
  - путем включения Рекомендаций в предоставляемый получателю финансовой услуги пакет документов при оказании ему финансовой услуги;
- 2) Включает в договор оказания финансовой услуги взаимное обязательство организации и клиента о соблюдении мер по защите имеющейся у них конфиденциальной информации от несанкционированного доступа и положение об уведомлении клиента о рисках использования информации в незаконных финансовых операциях;
- 3) Бесплатно консультирует своих клиентов по правовым и техническим вопросам защиты информации либо рекомендует им обращаться по этим вопросам в специализированные организации;
- 4) В отношении клиентов, ранее не уведомленных о рисках путем раскрытия информации в местах оказания услуг или путем уведомления в заявлении или в договоре, организация осуществляет уведомление при обращении клиента в организацию за услугой;
- 5) Немедленно прекращает дистанционное обслуживание клиента, а также любой обмен с ним конфиденциальными электронными сообщениями по телекоммуникационным каналам, в случае получения информации об утрате клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовых операций;
- 6) Направляет электронные сообщения на электронные адреса, номера телефонов, указанные в договоре с клиентом и обрабатывает сообщения, полученные с таких номеров