|  |  |
| --- | --- |
|  | Приложение к приказуГенерального директора ООО «ММК Меркада»От 20.03.2024 г № 8 |

**ПРАВИЛА**

**ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ И ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА**

**ООО МКК «Меркада»**

1. **ТЕРМИНЫ И ОПРЕЛЕНИЯ**

Стороны установили, что для настоящего Соглашения действуют следующие термины и определения:

* 1. **Авторизация** – процесс анализа МФО введенных Участником идентификационных данных, по результатам которого в отношении Участника определяется объем прав на использование Системы ДО и устанавливается принадлежность Участнику предъявленной им ПЭП, которая дала положительный результат при ее проверке МФО. Виды идентификационных данных определяются МФО;
	2. **Аутентификация** – проверка принадлежности Участнику электронного взаимодействия предъявленного им идентификатора, подтверждение подлинности идентификатора.
	3. **Доверенный канал** – это канал связи, который обеспечивает аутентификацию источника передаваемых данных, их конфиденциальность и контроль целостности, исключающие возможность подмены данных.
	4. **Журнал событий** – электронный документ, представляющий собой содержание лог-файла по учету действий (активности) Клиента в Системе ДО МФО, фактов подписания Клиентом электронных документов ПЭП;
	5. **Клиент** – физическое лицо, которое является потребителем финансовых услуг МФО и участником электронного взаимодействия, обратившийся в МФО с намерением получить или получившее финансовую услугу МФО. Клиент для целей настоящего Соглашения может именоваться – «**Заемщик»**;
	6. **Личный кабинет** – индивидуальный информационный раздел Клиента в закрытой части Сайта МФО, в мобильном приложении, созданный в процессе Регистрации, доступ к которому осуществляется по защищенному соединению. Личный кабинет позволяет Клиенту получать доступ к статической информации исполнения договора займа (заключенные электронные документы; история оплаты; текущая задолженность и др.). Доступ в Личный кабинет Клиента осуществляется путем сопоставления учетных данных Логина и Пароля от Личного кабинета Клиента (аутентификации), при этом:

**Логин** – символьное обозначение, используемое для идентификации Клиента в целях предоставления ему доступа к Личному кабинету. Логин совпадает с зарегистрированным в Системе ДО основным номером мобильного телефона Клиента либо адресом электронной почты Клиента;

**Пароль** – уникальная последовательность случайных букв, и/или чисел, и/или иных символов, используемых для аутентификации Клиента.

* 1. **МФО** – Общество с ограниченной ответственностью Микрокредитная компания «\*\*\*», сокращенное наименование ООО МКК «\*\*\*», ОГРН \_\_\_\_\_, ИНН \_\_\_\_, регистрационный номер в реестре МФО Банка России \_\_\_\_, адрес местонахождения: \_\_\_; контактный телефон: 8-\*\*\*-\*\*\*-\*\*\*\*), участник электронного взаимодействия, являющееся оператором Системы ДО и поставщиком финансовых услуг. МФО для целей настоящего Соглашения ПЭП может именоваться – «**Займодавец»**.
	2. **Основной номер мобильного телефона (далее – «ОМТ») –** абонентский номер Участника электронного взаимодействия в сети телефонной сотовой связи, предоставленный Участнику оператором сотовой связи, зарегистрированным и действующим на территории Российской Федерации в порядке, предусмотренном законодательством Российской Федерации, указанный и подтвержденный Участником в процессе Регистрации в Системе ДО МФО;
	3. **Адрес электронной почты Участника (e-mail)** – адрес электронной почты, владельцем которой является только Участник электронного взаимодействия.
	4. **Простая электронная подпись (далее - «ПЭП») –** электронная подпись Клиента, которая посредством использования Кодов подтверждения, паролей, иных средств идентификации подтверждает факт формирования электронной подписи определенным лицом, т.е. позволяющей МФО однозначно определить Клиента при подписании документов, в том числе договора комплексного обслуживания физических лиц, Заявления; Согласия; договора потребительского займа и др. ПЭП признается аналогом собственноручной подписи Клиента. Код отправляется МФО в виде SMS-сообщения на основной номер мобильного телефона Клиента, указанный Клиентом в качестве основного контактного;
	5. **Регистрация в Системе дистанционного обслуживания и электронного документооборота (далее – «Регистрация») –** присвоение учетной записи Клиенту, в результате добровольного предоставления последним своих персональных данных, необходимая для его опознания (аутентификации) и предоставления доступа к личным данным, которые хранятся в Системе ДО МФО. Регистрация осуществляется в целях создания Личного кабинета на официальном Сайте МФО, подачи онлайн Заявления на предоставление потребительского займа;
	6. **Сайт** – официальные сайты МФО в сети Интернет, расположенные по адресу: <https://___.ru>. Сайт МФО представляет собой информационную систему по предоставлению финансовых услуг физическим лицам. Доступ к Сайту МФО осуществляется с использованием защищенного SSL-соединения, организуемого посредством сертификатов Thawte;
	7. **Система дистанционного обслуживания и электронного документооборота (далее - «Система ДО» либо «Система»)** - совокупность программ, технических средств, используемых МФО при осуществлении деятельности по предоставлению потребительских займов Клиентам;
	8. **Участники электронного взаимодействия (далее – «Участники»)** – МФО, Агент и Клиент при совместном упоминании, являющиеся Сторонами Соглашения об обмене электронными документами с использованием Системы ДО, осуществляющие обмен информацией в электронной форме. Участники электронного взаимодействия для целей настоящих Правил могут именоваться – «**Стороны»**;
	9. **Электронный документ** – совокупность данных, которые обрабатываются и хранятся в электронной вычислительной машине и могут передаваться по системе телекоммуникаций или на магнитных носителях. Электронный документ может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего Электронного документа осуществляется воспроизводство содержания документа вместе с Электронной подписью. Все экземпляры Электронного документа являются подлинниками данного Электронного документа;
	10. **Электронный документооборот** (далее – «**ЭДО**») – обмен в информационной системе электронными документами между МФО и Участниками электронного взаимодействия, а также между отдельными Участниками в соответствии с настоящими Правилами.

Настоящие Правила содержат также иные термины (и их сокращения), которые используются в значениях, определенных в соответствующих разделах Правил.

Иные термины, используемые в Правилах, применяются в значениях, определяемых действующим законодательством Российской Федерации (далее – «**РФ**»), в том числе, Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее по тексту – Закон № 63-ФЗ), Соглашением об использовании простой электронной подписи, Соглашением об обмене электронными документами с использованием Системы ДО.

1. **ПРЕДМЕТ РЕГУЛИРОВАНИЯ НАСТОЯЩИХ ПРАВИЛ**
	1. Настоящие Правила устанавливают общий порядок электронного документооборота в Системе дистанционного обслуживания и электронного документооборота МФО, порядок формирования ключей электронной подписи и осуществления МФО иных функций, предусмотренных настоящими Правилами, в рамках соответствующей Системы ДО.

Система ДО – система, предназначенная для осуществления взаимодействия между:

* МФО и Участниками в области оказания МФО финансовых услуг по предоставлению потребительских микрозаймов;
* Отдельными Участниками в области, не связанной с оказанием МФО финансовых услуг по предоставлению потребительских микрозаймов.
	1. Настоящие Правила содержат условия соглашения, налагающего обязательства и устанавливающего ответственность сторон, вовлеченных в процесс Электронного документооборота.
	2. Соглашение об использовании простой электронной подписи и электронном документообороте (далее – «**Соглашение ПЭП**») заключается путем присоединения Участника к установленным настоящими Правилами условиями в целом в следующем порядке:
		1. Лицо, желающее заключить с МФО Соглашение об ПЭП и удовлетворяющее требованиям МФО, совершает полное и безоговорочное принятие настоящих Правил и предложения МФО заключить Соглашение ПЭП (оферты) путем выполнения действий, указанных в оферте (акцепт).
1. **ПОРЯДОК ДЕЙСТВИЯ НАСТОЯЩИЙ ПРАВИЛ**
	1. Настоящие Правила, включая все приложения, а также изменения и дополнения к ним, утверждаются в одностороннем порядке по решению МФО, которое вправе определить сроки и порядок вступления в силу изменений и дополнений в настоящие Правила и приложения к ним.
	2. МФО вправе по своему усмотрению отказаться от заключения Соглашения ПЭП с лицом, имеющим намерение стать Участником электронного взаимодействия.
	3. Действующая редакция настоящих Правил размещена на официальном Сайте МФО в сети «Интернет». Изменения и дополнения к настоящим Правилам и приложениям к ним, а также решения МФО о сроках и порядке вступления их в силу, доводятся до сведения Участников путем размещения на официальном Сайте МФО в сети «Интернет» не позднее, чем за 3 (три) рабочих дня до вступления в силу таких изменений в Правила и решений МФО.
	4. Настоящие Правила прекращают свое действие на основании решения МФО. В случае прекращения действия Правил МФО уведомляет об этом за 30 (тридцать) календарных дней до даты прекращения действия Правил.
	5. Прекращение действия настоящих Правил и приложений к ним не влияет на юридическую силу и действительность Электронных документов, которыми МФО, Участники электронного взаимодействия обменивались до прекращения действия настоящих Правил и приложений к ним.
2. **ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ДО**
	1. Система ДО представляет собой защищенное приложение, обеспечивающее безопасный обмен через Интернет Электронными документами между МФО, физическими и юридическими лицами (Участниками).
	2. Передача Электронных документов осуществляется исключительно в рамках Системы ДО.
	3. Достоверность и целостность Электронных документов в Системе ДО обеспечивается фактом формирования Клиентом электронной подписи при обмене Электронными документами в Системе ДО (подтверждается простой электронной подписью).
	4. Условиями допуска юридических и физических лиц к осуществлению ЭДО является заключение Соглашения ПЭП либо договора потребительского микрозайма, в рамках которого предусмотрен обмен с МФО документами в электронном виде, подписанными электронной подписью, в случае обмена Электронными документами между отдельными Участниками в области, не связанной с оказанием МФО финансовых услуг по предоставлению потребительских микрозаймов, необходимым условием является также заключение Участниками с МФО отдельного Соглашения об обмене электронными документами с использованием Системы ДО.
3. **ИСПОЛЬЗОВАНИЕ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ**
	1. Простой электронной подписью (далее «**ПЭП**») является электронная подпись, которая посредством использования идентификаторов и паролей к ним, предназначенных для аутентификации в Системе ДО, идентификаторов и одноразовых паролей либо иной информации, включающей ключевую информацию, участвующую в аутентификации в Системе ДО, подтверждает факт формирования электронной подписи Участником или его уполномоченным лицом.
	2. Электронный документ считается исходящим от Участника, если он содержит реквизиты Участника предназначенные для аутентификации в Системе ДО.
	3. Риск неправомерного подписания электронного документа электронной подписью несет Участник, от имени которого данный документ подписан.
	4. Электронный документ, подписанный от имени Участника, не влечет правовых последствий, если до момента получения данного документа адресат будет уведомлен об аннулировании или блокировке идентификаторов/ иной информации, включающей ключевую информацию, участвующую в аутентификации в Системе ДО.
	5. Применение положений Правил, относящихся к электронному документу, подписанному простой электронной подписью с использованием одноразового пароля, распространяется также на каждый Электронный документ, входящий в состав пакета Электронных документов, подписанного простой электронной подписью с использованием одноразового пароля.
4. **ТРЕБОВАНИЯ К ЭЛЕКТРОННОМУ ДОКУМЕНТУ**
	1. Электронный документ, сформированный в Системе ДО, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в случае его надлежащего оформления в соответствии с настоящими Правилами.
	2. Электронный документ должен быть сформирован в определенном формате и подписан электронной подписью.
	3. Электронные документы, оформленные, переданные и/или полученные в соответствии с настоящими Правилами, признаются равнозначными документам на бумажных носителях, подписанным собственноручной подписью, и не могут быть оспорены только на том основании, что они совершены в электронном виде.
	4. Одной простой электронной подписью с использованием одноразового пароля может быть подписан пакет Электронных документов, состоящий из нескольких Электронных документов, выведенных одновременно в графический пользовательский интерфейс для просмотра и подписания электронных документов.

При подписании простой электронной подписью с использованием одноразового пароля Электронных документов каждый из Электронных документов, входящий в этот пакет, считается подписанным простой электронной подписью.

1. **СТАТУС ЭЛЕКТРОННОГО ДОКУМЕНТА**
	1. Статус Электронного документа – информация о текущем состоянии Электронного документа в Системе ДО, показывающая на каком этапе обработки находится Электронный документ. Текущее состояние Электронного документа отражается в Системе ДО посредством изменения статуса Электронного документа. Для получения актуального статуса Участнику требуется выполнить операцию обновления отображения информации в Системе ДО при помощи штатных средств обновления.
	2. Статус Электронного документа считается доведенным до сведения Участника не позднее дня, следующего за днем последнего изменения статуса в Системе ДО.
	3. Учет статусов Электронных документов ведется в Журнале событий Системы ДО.
2. **ПОДЛИННИК ЭЛЕКТРОННОГО ДОКУМЕНТА**
	1. Электронный документ может иметь неограниченно количество экземпляров. Для создания дополнительного экземпляра существующего Электронного документа осуществляется воспроизведение содержания документа вместе с Электронной подписью.
	2. Все экземпляры Электронного документа являются подлинниками данного Электронного документа.
	3. Электронный документ не может иметь копий в электронном виде.
	4. Подлинник Электронного документа считается не существующим в случаях если:
* Нет ни одного учтенного экземпляра данного Электронного документа;
* Получение или восстановление экземпляра Электронного документа невозможно;
* Нет способа установить подлинность электронной подписи.
	1. Копии Электронного документа могут быть изготовлены (распечатаны) на бумажном носителе, заверены собственноручной подписью и печатью (при наличии) МФО.
	2. Копии Электронного документа на бумажном носителе должны содержать обязательную отметку, свидетельствующую о том, что это копия.
	3. Электронный документ и его копии должны быть аутентичными.
	4. Программные средства, осуществляющие преобразование Электронного документа для изготовления (распечатки) в виде бумажного документа, являются неотъемлемой составной частью программного обеспечения, используемого в Системе ДО.
	5. Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности Электронного документа (если применимо), его соответствия установленному формату.
1. **АУТЕНТИФИКАЦИЯ УЧАСТНИКОВ СИСТЕМЫ ДО**
	1. В Системе ДО при использовании простой электронной подписи возможны следующие способы аутентификации:
* По идентификатору и паролю;
* По идентификатору и одноразовому паролю.

Для усиления безопасности возможно использование одновременно двух способов аутентификации.

* 1. МФО является оператором выдачи идентификаторов аутентификации и паролей к ним, а также обеспечивает функционирование систем одноразовых паролей и систем аутентификации Системы ДО, осуществляет создание (замену) идентификаторов и паролей к ним, а также выполняет все необходимые операции, связанные с обеспечением инициализации и безопасности систем одноразовых паролей и систем аутентификации Системы ДО.
	2. Участник может получить идентификаторы аутентификации и пароли к ним в результате успешной процедуры регистрации в Системе ДО, т.е. присвоения учетной записи Участнику, в результате добровольного предоставления последним своих персональных данных, необходимых для его идентификации. Регистрация осуществляется в целях создания Личного кабинета на официальном Сайте МФО.
	3. Участник при наличии технической возможности вправе самостоятельно производить замену паролей к идентификаторам аутентификации, а также производить операции смены информации, предназначенной для его аутентификации в Системе ДО.
	4. Создаваемый пароль должен соответствовать следующим требованиям:
* Содержать не менее 8 символов;
* Содержать буквенные и (или) цифровые символы.
	1. Участник обязан:
* Хранить в тайне пароли, в том числе одноразовые пароли, полученные посредством СМС-уведомлений на ОМТ Участника/электронной почты, идентификаторы и информацию, предназначенную для аутентификации в Системе ДО, принимать все возможные меры, предотвращающие нарушение их конфиденциальности;
* Не передавать третьим лицам SIM-карту с ОМТ Участника во избежание нарушения конфиденциальности;
* Осуществлять действия направленные на формирование ПЭП с использованием идентификаторов и паролей аутентификации и информации для аутентификации, полученной в порядке, установленном настоящими Правилами;
* В случае нарушения конфиденциальности паролей и идентификаторов аутентификации или информации, предназначенной для аутентификации в Системе ДО или их утери незамедлительно уведомить об этом МФО.
	1. Участник несет ответственность:
* За предоставление некорректного (не существующего или не принадлежащего Участнику) ОМТ Участника;
* За предоставление некорректного (не существующего или не принадлежащего Участнику) адреса электронной почты Участника;
* За несвоевременное информирование МФО, в том числе за возможные последующие негативные события, произошедшие в результате компрометации ключевой информации и/или паролей для доступа в Систему ДО.
1. **ПОРЯДОК И ПРАВИЛА НАПРАВЛЕНИЯ УЧАСТНИКУ ОДНОРАЗОВОГО ПАРОЛЯ**
	1. Одноразовые пароли посредством СМС-уведомления направляются только Участнику, выразившему свое согласие на получение СМС-уведомлений. Факт согласия на получение СМС-уведомлений подтверждается запросом на получение одноразового пароля на указанный для направления одноразовых паролей ОМТ при совершении физическим лицом действий, необходимых для принятия оферты МФО на заключение Соглашения ПЭП (акцепта).
	2. МФО в обязательном порядке обеспечивает фиксацию фактов отправки и доставки адресату одноразовых паролей посредством СМС-уведомления на ОМТ Участника. Факт отправки и доставки СМС-уведомления подтверждается детализацией СМС-уведомления (информация о дате и времени отправки СМС-уведомления, текст отправленного СМС-уведомления, дата и время доставки СМС-уведомления Участнику), которая указывается в технической информационной системе МФО и может быть предоставлена в случае возникновения спорной ситуации.
	3. Подписание (пакета) Электронных документов с использованием полученного посредством СМС-уведомления одноразового пароля осуществляется в личном кабинете Участника на официальном Сайте МФО в сети «Интернет».
	4. МФО вправе отказать в регистрации ОМТ Участника в следующих случаях:
* Если при проверке реквизитов Участника обнаружено указание Участником несуществующих/некорректных данных (номера телефона, договора, адреса электронной почты, ФИО/паспортные данные) и иных подобных реквизитов;
* Если при проверке реквизитов Участника обнаружено, что указанный ОМТ/адрес электронной почты уже зарегистрированы в Системе ДО за другим Участником;
* В случае нарушения Участником настоящих Правил.

Об отказе принятия сведений и/или документов от Участника, МФО информирует Участника.

* 1. МФО не несет ответственность за корректность (существование и принадлежность Участнику) ОМТ/адреса электронной почты Участника.
	2. МФО не несет ответственность за нарушение обязательств вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора.
1. **ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ**
	1. В ходе использования ПЭП и аутентификационных данных возможно возникновение конфликтных (спорных) ситуаций, связанных с формирование, доставкой, получением, подтверждением Электронных документов, а также с использованием электронной подписи в Электронных документах. Причиной конфликтной ситуации может служить:
* Оспаривание факта формирование Электронного документа;
* Оспаривание авторства Электронного документа (подозрение на нарушение процедуры идентификации Участника, сформировавшего Электронный документ);
* Оспаривание целостности Электронного документа (подозрение на нарушение свойства целостности Электронного документа при его передаче по каналу связи);
* Оспаривание факта отправления и/или получения Электронного документа;
* Оспаривание времени отправления и/или получения Электронного документа;
* Иные случаи возникновения конфликтных ситуаций.

Конфликтные ситуации разрешаются в рабочем порядке.

* 1. Подтверждение подлинности ПЭП осуществляется проверкой факта получения Участником аутентификационных данных для входа в Систему ДО, наличием записей входа в Систему ДО с предоставленными Участнику аутентификационными данными, существованием записей о формировании запроса в логе Системы ДО, наличием записей о факте отправки и ввода одноразовых паролей.
	2. Проверка факта наличия записей входа в Систему ДО, отправки одноразовых паролей в Системе ДО, времени создания Электронного документа в Системе ДО осуществляется путем предоставления оператором Системы ДО выгрузки Журнала записей из информационной системы на указанную дату и время.
	3. Проверка подлинности ПЭП в Электронном документе происходит следующим образом:
* Определяется Участник.
* Определяется информационная система, в рамках которой была сформирована ПЭП.
* Определяются реквизиты Участника, предназначенные для его аутентификации в Системе ДО (идентификаторы аутентификации и информация, предназначенная для аутентификации Участника).
* Определяется Электронный документ и его реквизиты.
* Осуществляется запрос в Систему ДО по реквизитам Электронного документа.
* Осуществляется проверка извлеченного из Системы ДО Электронного документа.

Подлинность ПЭП в Электронном документе считается подтвержденной, если по итогам проверки извлеченный из системы ДО Электронный документ содержит реквизиты Участника, предназначенные для его аутентификации в Системе ДО.

При проверке подлинности ПЭП в случае использования одноразовых паролей, осуществляется сопоставление одноразового пароля, введенного Участником Системы ДО при подписании Электронного документа, и пароля, направленного Участнику СМС-уведомлением на ОМТ, зарегистрированный в МФО. При положительном результате проверки идентичности указанных одноразовых паролей и положительной аутентификации Участника, использовавшего данный идентификатор для подписания Электронного документа, подлинность ПЭП считается подтвержденной.

1. **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ**
	1. Система обеспечения информационной безопасности.
		1. Электронные документа, участвующие в Электронном документообороте, и средства электронной подписи являются конфиденциальной информацией.
		2. Участники обязаны соблюдать меры по обеспечению информационной безопасности при организации Электронного документооборота. Соблюдение требований информационной безопасности при организации Электронного документооборота обеспечивает:
* Конфиденциальность информации (при передаче данных конфиденциальность обеспечивается функцией шифрования);
* Целостность передаваемой информации;
* Аутентификацию (передаваемую информацию может получить только лицо, кому она предназначена, а отправителем является именно тот, чьего имени она отправлена);
* Неотказуемость от передачи Электронного документа (невозможность отрицания факта отправления или получения передаваемой информации обеспечивается подписанием документа отправителем с использованием функций Электронной подписи и хранением принимающей стороной документа с электронной подписи в течение установленного срока).
	+ 1. Основные мероприятия по обеспечению информационной безопасности разделяются на применение аппаратно-программных средств и применение организационных мер.

К аппаратно-программным средствам относятся:

* Программные средства, специально разработанные для осуществления Электронного документооборота;
* Средства аутентификации и разграничения доступа;
* Средства антивирусной защиты, включая средства обеспечения безотказной работы.

К организационным мерам относятся:

* Размещение аппаратно-программных средств в помещении с контролируемым доступом;
* Административные ограничения доступа к этим средствам, допуск только специально подготовленных и уполномоченных лиц;
* Защита от повреждающих внешних воздействий (пожар и т.д.).
	1. Компрометация пароля для доступа в Систему ДО.
		1. Под компрометацией пароля понимается утрата доверия к тому, что пароль известен только его владельцу.
		2. К событиям, относящимся к явной компрометации пароля, могут быть отнесены следующие:
* Для Участников – юридических лиц: увольнение уполномоченных сотрудников, имевших доступ к паролю;
* Нарушение правил хранения и/или уничтожения пароля;
* Раскрытие пароля в разговоре (в том числе при общении с сотрудником МФО);
* Выбытие из владения помимо воли Участника ОМТ (в том числе, SIM-карта ОМТ), используемого Участником для получения СМС-уведомлений;
* Информация, получаемая на ОМТ Участника, стала доступной третьим лицам (в случае направления Участнику СМС-уведомлений).

При наступлении одного из вышеперечисленных событий, отнесенных к явной компрометации пароля, Участнику необходимо незамедлительно сообщить об этом МФО.

* + 1. К неявной компрометации пароля могут быть отнесены следующие события:
* Возникновение подозрений на утечку информации о пароле, хранящемся владельцем на оборудовании (например, в случае обнаружения вирусного заражения средствами антивирусной защиты, установки нелицензированного программного обеспечения, передачу оборудования в сервисный центр и т.д.);
* Другие события, произошедшие при работе с паролем (например, при работе в общественных местах).

При наступлении одного из вышеперечисленных событий, отнесенных к неявной компрометации пароля, владельцу необходимо произвести оценку ситуации и самостоятельно принять решение по дальнейшему использованию пароля.