

Небанковская кредитная организация «МОНЕТА.РУ» (общество с ограниченной ответственностью) 424000, г. Йошкар-Ола, ул. Гоголя, д.2, стр. «А», тел. (8362) 45-43-83 ОГРН 1121200000316 ИНН/КПП 1215192632/121501001 БИК 048860734	Утверждено: Приказом № _____ от 31 мая 2016 г. Председатель Правления НКО «МОНЕТА.РУ» (ООО) _____ В.Р. Маймин
---	---

**ПРАВИЛА БЕЗОПАСНОСТИ В ОТНОШЕНИИ ИСПОЛЬЗУЕМЫХ СРЕДСТВ
ДОСТУПА К СЧЕТАМ ПРИ РАБОТЕ С ЭДС
НЕБАНКОВСКОЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ
«МОНЕТА.РУ» (общество с ограниченной ответственностью)**

(Версия 1.3)

Йошкар-Ола, 2016

СОДЕРЖАНИЕ

Контроль версий документа	3
Порядок пересмотра документа	3
1. Правила обеспечения безопасности автоматизированного рабочего места (АРМ)	3
2. Правила обеспечения безопасности при работе с ЭДС	4
3. Использование паролей в целях аутентификации клиента при осуществлении переводов ЭДС.....	4
4. Ограничения при переводе ЭДС.....	5

Контроль версий документа

Версия	Дата	Изменения
Версия 1.0	05.04.2013	Исходная версия.
Версия 1.1	15.07.2013	Изменено понятие «идентификация» на «аутентификация» в связи с неоднозначным чтением в контексте законодательства РФ.
Версия 1.2	15.02.2016	Изменения оформления документа в соответствии с корпоративным стандартом. Функциональные изменения не вносились.
Версия 1.3	31.05.2016	Дополнено разделами 3, 4

Порядок пересмотра документа

В целях постоянного совершенствования данного документа в соответствии с изменениями условий деятельности, законодательства, регулирующих требований, изменениями в организационной структуре или информационной инфраструктуре рекомендуется регулярно пересматривать данный документ – не реже одного раза в год. По результатам пересмотра в документ в случае необходимости вносятся соответствующие изменения.

Внеплановый пересмотр данного документа может быть выполнен в случае внесения существенных изменений в информационную инфраструктуру, а также по итогам расследования критичных инцидентов информационной безопасности.

1. Правила обеспечения безопасности автоматизированного рабочего места (АРМ)

1.1. Для выполнения процедуры аутентификации и авторизации доступа к счетам при работе с электронными денежными средствами (ЭДС) используйте только доверенные АРМ. Не используйте без крайней необходимости свой счёт в платёжной системе в различных интернет кафе и на компьютерах, к которым у вас нет доверия.

1.2. По возможности в качестве АРМ используйте выделенный компьютер, который будет выполнять только эту функцию. Альтернативным вариантом является использование виртуальной машины в рамках какой-либо системы виртуализации (например, VirtualBox, VMWare). В крайнем случае, постарайтесь минимизировать количество побочных функций, выполняемых АРМ для работы с ЭДС.

1.3. По возможности используйте межсетевой экран. Оборудование домашнего класса (SOHO) имеет невысокую стоимость, но является дополнительным уровнем защиты АРМ и существенно снижает риски.

1.4. Используйте средства антивирусной защиты. Регулярно обновляйте антивирусные базы и антивирусное программное обеспечение (ПО).

1.5. Используйте учетную запись с минимальным уровнем привилегий, необходимых для выполнения функций работы с ЭДС. Не используйте учетные записи с административными правами для повседневной работы.

1.6. Используйте стойкие пароли на всех уровнях защиты. Выбирайте пароль не менее 12 символов. Старайтесь использовать в пароле максимально возможное количество классов символов: строчные и прописные буквы, цифры, спецсимволы. Не используйте словарные пароли, а также словарные сочетания. Не используйте пароли, которые можно легко запомнить на слух или подсмотрев написание. Ни в коем случае не используйте пароли, которые могут быть получены путем анализа ваших персональных

данных: имена, клички животных, даты рождения, телефонные и автомобильные номера и т.д.

1.7. Регулярно меняйте пароли на всех уровнях защиты.

1.8. Строго следуйте условиям и соглашениям платёжной системы, не передавайте пароли и коды доступа посторонним лицам.

1.9. В случае обнаружение признаков заражения АРМ вредоносным ПО или подозрений о произошедшем несанкционированном доступе в систему дистанционного банковского обслуживания (ДБО) следует немедленно связаться со службой поддержки и заблокировать учетную запись до выяснения обстоятельств. Связаться со службой поддержки можно одним из способов, указанных на сайте <https://www.moneta.ru>.

2. Правила обеспечения безопасности при работе с ЭДС

2.1. Не используйте без крайней необходимости для работы с ЭДС подключения к сети, которым вы не можете доверять: в интернет-кафе, клубах, барах. Использование такого типа подключения не может быть определяющим фактором для несанкционированного доступа, но является дополнительным фактором риска.

2.2. Перед входом в систему ДБО, убедитесь, что вы перешли на адрес именно [https://www.moneta.ru/](https://www.moneta.ru) и соединились по защищенному соединению (https), при этом браузер не выдавал предупреждений об использовании недоверенного сертификата, либо сертификата который истек, отозван или выпущен для другого доменного имени.

2.3. Не сохраняйте пароли в браузерах. Средства запоминания паролей в популярных браузерах (Firefox, Chrome) сохраняют пароли на диске в открытом виде (Если не принято дополнительных мер для сохранения их в зашифрованном виде), откуда они могут быть легко скомпрометированы при заражении операционной системы вредоносным ПО.

2.4. Старайтесь не заходить на другие сайты параллельно работая в системе ДБО, а также не заходить на малознакомые сайты сомнительного содержания.

2.5. Будьте внимательны ко всем входящим письмам, SMS от имени платежной системы и системы ДБО. Текущие механизмы работы этих средств информирования не обеспечивают подлинности отправителя и могут быть использованы в различных схемах мошенничества.

2.6. Не сообщайте ваших паролей никому, даже службе поддержки и сотрудникам платежной системы. Для выполнения своих функциональных обязанностей нашим сотрудникам не нужно знать реквизитов доступа клиента. Если кто-то под каким-то предлогом пытается их узнать, скорее всего это мошенники.

3. Использование паролей в целях аутентификации клиента при осуществлении переводов ЭДС

3.1. Используемые одноразовые пароли однозначно соответствует сеансу использования системы или распоряжению клиента о переводе ЭДС, подтверждаемому клиентом с использованием системы, доводятся до клиента по альтернативным каналам связи или входят в набор возможных одноразовых паролей, которые доводятся до клиента или создаются клиентом с использованием технического средства, предназначенных для генерации одноразовых паролей.

3.2. До подтверждения клиентом распоряжения с использованием одноразового пароля система направляет клиенту по альтернативному каналу связи сообщение, содержащее сведения о сформированном с использованием системы распоряжении о переводе денежных средств, которое включает сумму и получателя денежных средств, при условии, что выбранный альтернативный канал обеспечивает такую возможность.

3.3. Для подтверждения клиентом права доступа в систему по умолчанию

аутентификационными данными являются логин и пароль. Дополнительно в целях повышения безопасности клиенту предоставляется возможность использовать одноразовый код подтверждения в целях аутентификации, получаемый следующим способом:

- одноразовый пароль TOTP (RFC 6238). Для входа используется пароль, который генерируется приложением на устройстве клиента. Новый пароль генерируется каждые 30 секунд и может быть использован только один раз.

3.4. Для подтверждения распоряжения о разовом переводе ЭДС или о распоряжении о периодических переводах денежных средств в определенную дату и (или) период, при наступлении определенных распоряжением условий клиент может использовать следующие способы:

- статический платежный пароль. Для проведения операций всегда используется один и тот же платежный пароль, срок действия не ограничен;

- последовательность по порядку. Распечатывается карточка со списком платежных паролей. При каждом проведении операции используется новый платежный пароль. Пароли выбираются из списка последовательно, общий срок действия не ограничен;

- SMS пароль. Для проведения операций используется платежный пароль, полученный в SMS сообщении. Пароль является одноразовым, и действует в течение 10 минут. Для проведения каждой операции Вам требуется получать новое SMS сообщение, содержащее пароль;

- SMS пароль (сессионный). Для проведения операций используется платежный пароль, полученный в SMS сообщении. В течение пользовательской сессии один и тот же пароль может использоваться несколько раз. В любой момент времени можно запросить новый пароль. После выхода из системы пароль становится недействительным.

- одноразовый платежный пароль TOTP (RFC 6238). Для проведения операций используется платежный пароль, который генерируется приложением на устройстве клиента. Новый платежный пароль генерируется каждые 30 секунд и может быть использован только один раз.

4. Ограничения при переводе ЭДС

4.1. На основании "Соглашения об использовании Электронного средства платежа «МОНЕТА.РУ» и о переводе электронных денежных средств" НКО определяет параметры операций которые могут осуществляться с использованием системы в том числе:

4.1.1. Максимальную сумму переводов ЭДС с использованием системы за одну операцию и (или) за определенный период времени которая устанавливается "Лимитами НКО «МОНЕТА.РУ» (ООО) на проведение операций";

4.1.2. Перечень возможных получателей ЭДС, в адрес которых клиентом могут быть совершены переводы ЭДС с использованием системы, который определяется "Лимитами НКО "МОНЕТА.РУ" (ООО) на проведение операций". Перечень получателей юридических лиц и индивидуальных предпринимателей, в том числе нерезидентов, доступен в Личном кабинете в виде каталога;

4.1.3. Перечень устройств, с использованием которых может осуществляться доступ к системе с целью осуществления переводов ЭДС, определяется клиентом в соответствующем разделе Личного кабинета на основе идентификаторов устройств;

4.1.4. Перечень IP-адресов, с использованием которых может осуществляться доступ к системе с целью осуществления переводов ЭДС, определяется клиентом в соответствующем разделе Личного кабинета.

4.1.5. Перечень услуг, предоставляемых с использованием системы который

перечислен в "Тарифах НКО «МОНЕТА.РУ» (ООО) на обслуживание физических лиц";
4.1.6. Временной период, в который могут быть совершены переводы ЭДС с использованием системы установлен в режиме 24 часа 7 дней в неделю.