| | |
|---|---|
| Небанковская кредитная организация<br>«МОНЕТА.РУ» (общество с ограниченной ответственностью)<br>424000, г.Йошкар-Ола, ул. Гоголя, д.2, стр. «А» , тел. (8362) 45-43-83<br>ОГРН 1121200000316<br>ИНН/КПП 1215192632/121501001<br>БИК 048860734 | Утверждено:<br>Приказом № 20/2 от «15» февраля 2016 г.<br>Председатель Правления<br>НКО «МОНЕТА.РУ» (ООО)<br>_____ В.Р. Маймин |

**ПРАВИЛА БЕЗОПАСНОСТИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ ПО ПРИЕМУ ПЛАТЕЖЕЙ ЗА ПРОДАННЫЕ ТОВАРЫ ИЛИ ОКАЗАННЫЕ УСЛУГИ НЕБАНКОВСКОЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ «МОНЕТА.РУ» (общество с ограниченной ответственностью)**

**(Версия № 1.2)**

**Йошкар-Ола, 2016**

## СОДЕРЖАНИЕ

## *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. |

## *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. Для входа в платежную систему запрещается использовать разделяемые учетные записи (одними аутентификационными данными пользуются несколько людей). При данном сценарии невозможно сопоставить действие в системе конкретному лицу, что влечет за собой множество рисков.

1.7. В настройках безопасности рекомендуется настроить ограничение входа в систему по IP-адресам, в случае если вы располагаете постоянным местом работы с фиксированным адресом. Данная мера существенно снижает риск несанкционированного доступа в случае компрометации пароля.

1.8. 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.

1.9. Регулярно меняйте пароли на всех уровнях защиты.

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

1.11. 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/ 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.