

| | |
|--|--|
| Небанковская кредитная организация «МОНЕТА» (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 № 22 от «31» января 2018 г. Председатель Правления НКО «МОНЕТА» (ООО) _____ В.Р. Маймин |
|--|--|

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

(Версия № 1.3)

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 |

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 | 31.01.2018 | Дополнено разделом 1.12. Изменены разделы 1.2, 2.2. |

Порядок пересмотра документа

Актуализация настоящих Правил проводится при возникновении следующих условий:

- существенных изменений в информационной инфраструктуре или организационной структуре Небанковской кредитной организации «МОНЕТА» (общество с ограниченной ответственностью) (далее - НКО);
- выявления инцидентов информационной безопасности, способных повлиять на процессы, описанные в настоящих Правилах;
- при появлении новых требований к обеспечению безопасности конфиденциальной информации, со стороны законодательства Российской Федерации, органов исполнительной власти Российской Федерации и Банка России.

По результатам пересмотра в документ в случае необходимости вносятся соответствующие изменения.

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). Данные подходы к организации АРМ позволяют минимизировать риски, связанные с несанкционированным изменением конфигураций АРМ. 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 платёжную 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 обнаружения 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>.

1.12. В случае утраты (потере или хищении) АРМ, используемого для работы с ЭДС, 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. В целях минимизации рисков, связанными с появлением в сети «Интернет» ложных (фальсифицированных) копий информационных ресурсов НКО, 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 платёжной 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.