НКО «МОНЕТА» (ООО) ИНН 1215192632, КПП 121501001 ОГРН 1121200000316, ОКПО 38024380	УТВЕРЖДЕНЫ Приказом Председателя Правления НКО «МОНЕТА» (ООО) от 27.03.2024 № 109

ПРАВИЛА
БЕЗОПАСНОСТИ ПРИ ДОСТУПЕ К СЧЕТАМ И СОВЕРШЕНИИ ОПЕРАЦИЙ ПО ПЕРЕВОДУ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ НЕБАНКОВСКОЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ «МОНЕТА» (общество с ограниченной ответственностью)

(Версия 1.0)

Йошкар-Ола

2024

СОДЕРЖАНИЕ

Контроль версий документа

Версия	Дата	Изменения
Версия 1.0	27.03.2024	Исходная версия. Взамен «Правил безопасности в отношении используемых средств доступа к счетам при работе с ЭДС небанковской кредитной организации» версии 1.4 и «Правил безопасности при совершении операций по приему платежей за проданные товары или оказанные услуги небанковской кредитной организации версии 1.3

1. Порядок пересмотра документа

Внесение изменений в Правила безопасности при доступе к счетам и совершении операций по переводу электронных денежных средств (далее – Правила) 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.

2. Правила обеспечения безопасности автоматизированного рабочего места

2.1 Для выполнения процедуры аутентификации и авторизации доступа к счетам при работе с электронными денежными средствами (далее – ЭДС) используйте только доверенные автоматизированные рабочие места (далее – АРМ). С целью минимизации компрометации используемого счета не используйте свой счёт в платёжной системе в различных интернет-кафе и на компьютерах, к которым у вас нет доверия.

2.2 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.

2.3 Требования к АРМ, на котором осуществляется работа с ЭДС:

- должна быть установлена только одна операционная система и только те программы, которые необходимы для работы с ЭДС;

- должны быть отключены все неиспользуемые для связи службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети и др.);

- операционная система, как и любое другое программное обеспечение (далее – ПО), должно быть только лицензионным и в актуальной версии;

-должны своевременно устанавливаться обновления операционной системы, а также обновления по безопасности прикладного ПО;

- должна быть активирована подсистема регистрации событий информационной безопасности;

- необходимо исключить использование специализированного ПО для удаленного администрирования («RAdmin», «TeamViewer», «Ammyy Admin») и другого ПО с подобным функционалом.

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

2.5 Доступ в сеть Internet разрешить только тем программам, которые необходимы для работы с ЭДС и запрещающие любые иные обращение к компьютеру из сети Internet.

2.6 Включенный АРМ не должен оставаться без контроля. Нельзя отлучаться от АРМ пока происходит электронный обмен данными. Время автоматической блокировки экрана во время бездействия пользователя должно составлять не более 3 минут. Разблокировка экрана должна происходить по паролю пользователя.

2.7 Используйте лицензионные средства антивирусной защиты (средства защиты от вредоносного кода). Регулярно обновляйте антивирусные базы и антивирусное ПО.

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

2.9 Используйте стойкие пароли на всех уровнях защиты. Выбирайте пароль не менее 16 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, то есть которые имеют смысловую нагрузку: имена, клички животных, даты рождения, телефонные и автомобильные номера и т.д.

2.10 Регулярно меняйте пароли на всех уровнях защиты АРМ, не реже чем один раз в 60 дней.

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

2.12 В случае обнаружение признаков заражения АРМ вредоносным ПО, компрометации пароля или подозрений о произошедшем несанкционированном доступе в систему дистанционного банковского обслуживания (далее – 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.

2.13 В случае утраты (потери 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.

3. Правила обеспечения безопасности при работе с ЭДС

3.1 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 https://www.moneta.ru/ и соединились по защищенному соединению (https). При правильном соединении появится значок

защищенного соединения («замок»). Браузер не должен выдавать предупреждений об использовании недоверенного сертификата либо сертификата, который истек, отозван или выпущен для другого доменного имени.

3.2 Не сохраняйте пароли в браузерах. Средства запоминания паролей в популярных браузерах (Firefox, Chrome и т.д.) 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.

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

3.4 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.

3.5 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.

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

4.1 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 технических средств, предназначенных для генерации одноразовых паролей.

4.2 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.

4.3 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 для 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.

4.4 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.

5. Ограничения при переводе ЭДС

5.1 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:

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

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

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

5.1.4 Перечень услуг, предоставляемых с использованием системы, который перечислен в «Тарифах НКО «МОНЕТА» (ООО) на обслуживание»;

5.1.5 Временной период, в котором могут быть совершены переводы ЭДС с использованием системы, установлен в режиме 24 часа 7 дней в неделю.