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

ПОРЯДОК
ДЕЙСТВИЙ В СЛУЧАЕ НАЛИЧИЯ ПОДОЗРЕНИЯ О КОМПРОМЕТАЦИИ СРЕДСТВ ДОСТУПА К СЧЕТУ НЕБАНКОВСКОЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ «МОНЕТА» (общество с ограниченной ответственностью)

(Версия № 1.3)

Йошкар-Ола
2024

СОДЕРЖАНИЕ

1. Контроль версий документа

Версия	Дата	Изменения
Версия 1.0	05.04.2013	Исходная версия.
Версия 1.2	31.01.2018	Изменения оформления документа в соответствии с корпоративным стандартом. Функциональные изменения не вносились.
Версия 1.3	27.03.2024	Удален п. 3.10. Изменена нумерация. Функциональные изменения не вносились.

2. Порядок пересмотра документа

Внесение изменений в Порядок действий в случае наличия подозрения о компрометации средств доступа к счету небанковской кредитной организации (далее – Порядок) 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 настоящем Порядке;
- 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.

3. Порядок действий в случае наличия подозрения о компрометации средств доступа к счету

3.1 Немедленно прекратить любые действия с учетной записью системы Дистанционного банковского обслуживания (далее – Системы). Также прекратить использование автоматизированного рабочего места (далее – АРМ), выключить его из сети в обход штатной процедуры завершения работы. В случае использования мобильных устройств выключить их с извлечением аккумулятора. При отсутствии возможности обесточивания АРМ выключить его через штатную процедуру.

3.2 Заблокировать учетную запись Системы, связавшись со службой поддержки Системы одним из способов, указанных на сайте https://www.moneta.ru (далее – сайт НКО). Для ускорения обработки заявки рекомендуется позвонить по телефону, указанному на сайте НКО.

3.3 Сообщить службе поддержки Системы о необходимости блокировки финансовых операций по счету. Указанное действие может сохранить ваши денежные средства от хищения.

3.4 Выполнить процедуру смены всей ключевой и парольной информации, обратившись в службу поддержки Системы.

3.5 Ни при каких обстоятельствах не отвечать на письма, якобы от имени Системы, с требованиями (просьбами, предложениями) зайти на сайт, внешне похожему, но не принадлежащему домену https://www.moneta.ru, и направить логин или пароль доступа к нему.

3.6 При наличии возможности провести сбор записей с межсетевых экранов и других средств защиты, серверов баз данных и иных компонентов.

3.7 При возможности оперативно обратиться к своему интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений как минимум за три месяца, предшествующих факту несанкционированного доступа, с целью установления факта неправомерного доступа к учетной записи.

3.8 В случае поступления на мобильный номер SMS-оповещения или электронного сообщения о совершенной операции, которая была инициирована не Вами, необходимо незамедлительно связаться со службой поддержки Системы одним из способов, указанных на сайте https://www.moneta.ru, и сообщить об этом.

3.9 Если вы планируете обратиться в правоохранительные органы с целью расследования инцидента, не предпринимайте никаких действий для самостоятельного или с привлечением ИТ-специалистов поиска и удаления вредоносного ПО.

3.10 По возможности все действия производить коллегиально, протоколировать и документировать, в том числе с использованием фотосъемки.

3.11 В случае хищения денежных средств со счета оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела.

3.12 Копии документов также необходимо направить в службу поддержки Системы для дальнейшего расследования инцидента.