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

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

(Версия № 1.2)

Йошкар-Ола, 2018

СОДЕРЖАНИЕ

Контроль версий документа

Версия	Дата	Изменения
Версия 1.0	05.04.2013	Исходная версия.
Версия 1.1	15.02.2016	Изменения оформления документа в соответствии с корпоративным стандартом. Функциональные изменения не вносились.
Версия 1.2	31.01.2018	Плановый пересмотр документа. Функциональные изменения не вносились.

Порядок пересмотра документа

Актуализация настоящего Порядка 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.

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

1. Немедленно прекратить любые действия с учетной записью системы ДБО. Также прекратить использование АРМ, выключить его из сети в обход штатной процедуры завершения работы. В случае использования мобильных устройств выключить его, извлечением аккумулятора. При отсутствии возможности обесточивания АРМ, выключить его через штатную процедуру.
2. Заблокировать учетную запись системы ДБО, связавшись со службой поддержки одним из способов, указанных на сайте https://www.moneta.ru. Для ускорения обработки заявки рекомендуется позвонить по телефону.
3. Сообщить службе поддержки о необходимости блокировки финансовых операций. При определенных обстоятельствах это может сохранить ваши денежные средства от хищения.
4. Выполнить процедуру смены всей ключевой и парольной информации, обратившись в службу поддержки.
5. При наличии возможности провести сбор записей с межсетевых экранов и других средств защиты, серверов баз данных и иных компонент.
6. 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.
7. 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.

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

9. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.

10. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения, а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения.

11. Копии документов направить в службу поддержки платежной системы.