Общество с ограниченной ответственностью
«Микрокредитная компания «БРИКС»
ИНН 9109019084 КПП 910201001

ПРИКАЗ № 10

г. Симферополь «30» июня 2023 г.

О реализации Положения
Банка России № 757-П

В связи с введением в действие Положения Банка России "ОБ СТАНОВЛЕНИИ ОБЯЗАТЕЛЬНЫХ ДЛЯ НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ФИНАНСОВЫХ РЫНКОВ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ОСУЩЕСТВЛЕНИЮ НЕЗАКОННЫХ ФИНАНСОВЫХ ОПЕРАЦИЙ" (утверждено Банком России 20 апреля 2021 г. N 757-П) и в целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков приказываю:

Осуществлять защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых Организацией (далее соответственно - автоматизированные системы, защищаемая информация, защита информации):

информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Организации (далее - электронные сообщения);

информации, необходимой Организации для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами или иным имуществом;

информации об осуществленных Организацией и его клиентами финансовых операциях;

ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемой Организацией и его клиентами при осуществлении финансовых операций (далее - криптографические ключи).

В случае если защищаемая информация содержит персональные данные, применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных".

1. Довести до клиентов Организации рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

Обеспечивать на протяжении всей деятельности Организации доведение до клиентов следующей информации:

о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

2. Обеспечение защиты информации с помощью СКЗИ осуществлять в соответствии с технической документацией на СКЗИ, а также следующими федеральными законами и нормативными правовыми актами Российской Федерации:

Федеральным законом от 6 апреля 2011 года № 63-ФЗ "Об электронной подписи" (далее - Федеральный закон "Об электронной подписи");

Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее - Федеральный закон "О персональных данных");

постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (далее - Положение ПКЗ-2005);

приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 "Об утверждении состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

3. В случае наличия в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований указанную оценку проводить в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

В случае применения СКЗИ российского производства, применять СКЗИ, имеющие сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

Обеспечить безопасность процессов изготовления криптографических ключей СКЗИ комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

4. Утвердить Политику информационной безопасности Организации (Приложение 1 к настоящему Приказу).
5. Настоящий Приказ вступает в силу с 1 июля 2023 г.
6. Контроль за исполнением Приказа возлагаю на себя.

Директор **О.А. Касатова**

Приложение № 1

к Приказу № 10 от 30.06.2023
г. «О реализации Положения
Банка России № 757-П»

Политика информационной безопасности

1. Общие положения

Настоящая политика информационной безопасности Организации с ограниченной ответственностью Микрокредитная компания «Брикс» (далее соответственно – «Организация», «Политика») предусматривает принятие необходимых мер в целях защиты активов Организации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник, при этом первоочередной задачей является обеспечение безопасности всех активов Организации. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив. Главные цели Организации не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники Организации. На лиц, работающих по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

1.1. Цель и назначение настоящей Политики

Целями настоящей Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам для поддержки деятельности;
- защита целостности деловой информации с целью поддержания возможности по оказанию услуг высокого качества и принятию эффективных управленческих решений;

- повышение осведомленности клиентов в области рисков, связанных с информационными ресурсами Организации;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной.

Ответственные сотрудники подразделений (при наличии таковых) должны обеспечить регулярный контроль за соблюдением положений настоящей Политики.

1.2. Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Организации. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Организации, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

Федеральные законы, изданные уполномоченными органами на их основе подзаконные акты, имеют приоритет над настоящей Политикой и изданными в соответствии с ней внутренними документами Организации в сфере информационной безопасности. В случае несоответствия внутренних документов Организации федеральным законам и (или) изданным уполномоченными органами на их основе подзаконным актам применяются соответствующие федеральные законы и (или) изданные уполномоченными органами на их основе подзаконные акты вне зависимости от того, внесены ли аналогичные положения во внутренние документы Организации.

Организации принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления им деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала.

1.3. Основные положения об обрабатываемой информации.

Организация осуществляет получение, подготовку, обработку, передачу и хранение информации со следующими ограничениями:

- Не совершает финансовых операций в электронном виде,
- Не направляет своим клиентам и не получает от своих клиентов документов (уведомлений, сообщений и т.п.) в электронном виде,
- Не осуществляет удалённой (дистанционной или иной, исключающей личное присутствие) авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами или иным имуществом,
- в силу совершения всех финансовых операций исключительно при личном контакте, при осуществлении финансовых операций Организация, его клиенты при осуществлении финансовых операций не используют средства криптографической защиты информации.

2. Требования и рекомендации

2.1. Ответственность за информационные активы

Ответственность за информационные активы несёт сотрудник, осуществляющий их получение, подготовку, обработку, передачу и хранение в автоматизированных системах.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения

Все работы в пределах офисов выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Организации.

Внос в здания и помещения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы производится только при согласовании с единоличным исполнительным органом Организации.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в информационную систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой, при этом максимальное время «простоя» компьютера до появления экранной заставки должно составлять не более 15 минут.

2.2.2. Доступ третьих лиц к системам.

Каждый сотрудник обязан немедленно уведомить единоличный исполнительный орган Организации обо всех случаях предоставления доступа третьим лицам к информационным ресурсам.

Доступ третьих лиц к информационным системам Организации должен быть обусловлен производственной необходимостью.

2.2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам Организации с учетом их взаимоотношений с ней.

Сотрудникам, использующим в работе портативные компьютеры Организации, может быть предоставлен удаленный доступ к сетевым ресурсам Организации (при наличии таковых).

Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Организации, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Организации и к каким-либо другим сетям, не принадлежащим Организации.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Организации, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.2.4. Доступ к сети Интернет

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности; при этом всеми сотрудниками Организации должны соблюдаться следующие ограничения:

- сотрудникам разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой

ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

- сотрудники не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Организации в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Организации;
- сотрудники перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Организации (при наличии таковой) для всех лиц, не являющихся сотрудниками.

Единоличный исполнительный орган Организации имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

2.3. Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Организации.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

2.3.1. Аппаратное обеспечение

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное Организацией, является его собственностью и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Организации, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства, не относятся к числу устройств, имеющих надежные механизмы защиты данных, в связи с чем хранение на них конфиденциальной информации не допускается.

2.3.2. Программное обеспечение

Все программное обеспечение, установленное на предоставленном Организацией компьютерном оборудовании, является собственностью

Организации и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно подлежит удалению.

Все компьютеры должны быть оснащены системой антивирусной защиты.

Сотрудники не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

Организация приобретает программное обеспечение, а не разрабатывает собственные программы.

2.4. Рекомендуемые правила пользования электронной почтой

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует основной деятельности.

Конфиденциальная информация не подлежит пересылке третьим лицам по электронной почте.

Сотрудники Организации для обмена документами с партнерами должны использовать только свой официальный адрес электронной почты.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Установлены следующие недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов, не связанных с деятельностью Организации;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит общепринятым стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в Организации процедурами документооборота.

2.5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте единоличному исполнительному органу Организации.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов.

- Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
- проинформировать единоличный исполнительный орган Организации;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Организации (при наличии таковой) до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.
-

2.6. Помещения с техническими средствами информационной безопасности

Конфиденциальные встречи (заседания) должны проходить только в защищенных помещениях.

Перечень защищённых помещений в каждом конкретном случае определяется единоличным исполнительным органом Организации.

Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с единоличным исполнительным органом Организации.

Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник, который отвечает за подготовку заседания, после получения разрешения единоличного исполнительного органа Организации.

Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

2.7. Управление сетью

Правила о корпоративной информационной сети Организации применяются в случае создания такой сети.

2.7.1. Ограничения на использование корпоративной информационной сети

Сотрудникам запрещается:

- нарушать информационную безопасность и работу сети;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу;
- передавать информацию о сотрудниках или списки сотрудников посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

2.7.2. Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах (при наличии таковых) только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

Все заявки на проведение технического обслуживания компьютеров должны направляться единоличному исполнительному органу Организации.

2.8. Внесение изменений в настоящую Политику

Изменения в настоящую Политику вносятся единоличным исполнительным органом Организации, в частности, в следующих случаях:

- изменение законодательства, подзаконных актов, вступление в силу частей законодательства, подзаконных актов с отложенным сроком вступления в силу;

- изменение масштабов деятельности, вызывающее необходимость изменения объёма, и (или) способов, и (или) технологии обработки информации;
- выявление уязвимостей защиты информации в Организации.