УТВЕРЖДАЮ
Генеральный директор
ТОО "МФО "Смартолёт Финанс"

_____ / Сейтбеков А.М.
Приказ № 07-ОД от "26" апреля 2023 года

ПРОЦЕДУРЫ
безопасности и защиты информации от несанкционированного доступа при предоставлении услуг МФО посредством интернет-ресурса www.aqsha.smartolet.kz

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Процедуры безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса в ТОО «МФО «Смартолёт Финанс» (далее – Процедуры) разработаны в соответствии с нормами действующего законодательства Республики Казахстан в сфере информационной безопасности, актами уполномоченного органа и внутренними документами ТОО «МФО «Смартолёт Финанс» (далее - МФО).
2. Основной целью Процедуры, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму. Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам МФО. С этой целью необходимо поддерживать главные свойства информации, а именно:
   - доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;
   - конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
   - целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
3. Основными принципами Процедуры являются:
   - законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации МФО;
   - ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности МФО;
   - непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты МФО должны осуществляться без прерывания или остановки текущих бизнес-процессов МФО;
   - комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
   - обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне

развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;
- приоритетность – категорирование (ранжирование) всех информационных ресурсов МФО по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности.

4. Настоящие Процедуры определяют:
- Основные меры по обеспечению информационной безопасности МФО;
- Бизнес процесс многофакторной аутентификации и верификации потенциальных заемщиков посредством интернет-ресурса;
- Программно-технические средства защиты информации от несанкционированного доступа при предоставлении услуг МФО посредством интернет-ресурса;
- Описание функционала и техническая характеристика Программного обеспечения по распознаванию удостоверяющих документов;
- Обеспечение безопасного хранения электронных сообщений и иных документов, предоставленных заемщику и полученных от него, с соблюдением их целостности и конфиденциальности в течение не менее 5 (пяти) лет после прекращения обязательств сторон по договору о предоставлении микрокредита;
- Меры для профилактики замышляемых правонарушений со стороны третьих лиц.

5. Настоящие Процедуры обязательны для исполнения всеми работниками МФО, стажерами, практикантами, а также должна доводиться до сведения заемщиков и иных третьих лиц, имеющих доступ к информационным системам и документам МФО, в той их части, которая непосредственно взаимосвязана с МФО и их деятельностью.

6. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды.

ГЛАВА 2. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7. Основными мерами по обеспечению информационной безопасности МФО являются:
- административно-правовые и организационные меры;
- меры физической безопасности;
- программно-технические меры.

7.1 Административно-правовые и организационные меры включают (но не ограничены ими):
- контроль исполнения требований законодательства РК и внутренних документов;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Процедуры;
- контроль соответствия бизнес-процессов требованиям Процедуры;
- информирование и обучение работников МФО работе с информационными системами и требованиям информационной безопасности;
- реагирование на инциденты, локализацию и минимизацию последствий;
- анализ новых рисков информационной безопасности;
- отслеживание и улучшение морально-делового климата в коллективе;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников МФО.

7.2 Меры физической безопасности включают (но не ограничены ими):
- организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
- организацию противопожарной безопасности охраняемых объектов;

- контроль доступа работников МФО в помещения ограниченного доступа (сервер).

7.3 Программно-технические меры включают (но не ограничены ими):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра (firewall, IPS и т.п.);
- применение комплексной антивирусной защиты;
- использование средств информационной безопасности,встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей, в первую очередь, привилегированных;
- применение систем криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств.

ГЛАВА 3. БИЗНЕС ПРОЦЕСС МНОГОФАКТОРНОЙ АУДЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА

8. Многофакторная аутентификация и верификация посредством интернет-ресурса www.aqsha.smartolet.kz включает в себя:

- Смс - сообщение;
- Система определения живости пользователя «VeriLive»;
- Система распознавания удостоверяющих документов «VeriDoc»;
- Система распознавания лиц «VeriFace».

9. Бизнес процесс многофакторной аутентификации и верификации интернет-ресурса www.aqsha.smartolet.kz осуществляется следующим образом:

9.1. На интернет-ресурсе www.aqsha.smartolet.kz потенциальный заемщик заполняет заявку на получение микрокредита, путем ввода ИИН, ФИО, а также номера мобильного телефона, для отправки смс-сообщения с уникальным кодом, который действует в течение 1-ой минуты. Код в свою очередь вводится на вкладке «Регистрация» на интернет-ресурсе www.aqsha.smartolet.kz, тем самым активируя личный кабинет заемщика. Данное действие подтверждает, что заемщик имеет при себе данный номер и имеет полный доступ к нему.

9.2. После активации и получения доступа в личный кабинет на интернет-ресурсе www.aqsha.smartolet.kz, потенциальному заемщику необходимо сфотографироваться, обязательно направив взгляд на камеру мобильного телефона. При этом, необходимо снять очки и головной убор.

9.3. В момент получения фотографии производится видеосъемка лица и потенциального заемщика и идет поиск изменении показателей мимики в биометрии лица перед камерой и сравниваются общие биометрические особенности лица в видео с фотографией. Это служит доказательством того, что полученная фотография заемщика сделана через программное обеспечение "Система определения живости «**VeriLive**» с образа живого, двигающегося человека.

9.4. Следующим действием осуществляется сканирование удостоверения личности через программное обеспечение «**VeriDoc**». Документ (удостоверение личности) фотографируется через камеру мобильного телефона, после чего сканируется с двух сторон.

9.5. После получения изображения документа (удостоверения личности) заемщика, программное обеспечение «**VeriFace**» осуществляет проверку его подлинности. Распознавание ключевых данных, таких как ИИН гарантируется наличием проверочной цифры в зоне MRZ документа.

9.6. Полученную информацию интернет-сайт www.aqsha.smartolet.kz отправляет в ТОО «Первое кредитное бюро» (далее - ПКБ) на предмет проверки потенциального заемщика по имеющейся базе данных.

9.7. В случае получения положительной информации от ПКБ, МФО принимает решение о выдаче микрокреита.

ГЛАВА 4. ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ МФО ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА

9. Программно-технические средства защиты информации от несанкционированного доступа при предоставлении услуг МФО посредством интернет-ресурса www.aqsha.smartolet.kz базируются на двух основных составляющих:
   1) организация топологии сети. На сервере, к которому открыт доступ из глобальной сети Интернет, конфиденциальная информация не хранится. Для этого сервер распределения ключей и база данных, содержащая информацию для обслуживания заемщиков, выносятся в отдельный сегмент сети, к которому невозможен доступ из глобальной сети;
   2) обеспечение безопасного обмена данными между заемщиком и сервером, доступным из глобальной сети. Для этого используются алгоритмы шифрования трафика, которые позволяют исключить ситуацию подмены сервера, раннее выявление недостатков в системе безопасности путем сопоставления протоколов обмена сообщениями на стороне заемщика и сервера. В случае обнаружения несовпадений транзакция отменяется, а ключ пользователя (или сервера) считается невалидным.
10. Конфиденциальность передаваемой информации обеспечивается шифрацией данных (SSL – англ. Secure Sockets Layer — протокол защищенных сокетов). Целостность передаваемой информации обеспечивается хешированием каждого SSL пакета.
11. Доступ к Интернет-ресурсу www.aqsha.smartolet.kz осуществляется посредством подключения к сайту www.aqsha.smartolet.kz по защищенному протоколу HTTPS.
12. Адрес в сети Интернет – www.aqsha.smartolet.kz принадлежит МФО. МФО гарантирует пользователям сервисов интернет-ресурса «wwww.aqsha.smartolet.kz» защиту их персональных и платежных данных.
13. Программно-технический комплекс интернет-ресурса www.aqsha.smartolet.kz выделен в отдельную защищенную подсеть.
14. Допуск заемщика в личный кабинет осуществляется после его идентификации и аутентификации. Для регистрации заемщика в личном кабинете требуется ИИН заемщика.
15. Идентификация и аутентификации заемщика осуществляется МФО путем проверки правильности указания заемщиком:

15.10. при регистрации заемщика – ИИН и номер мобильного телефона заемщика;

15.11. при входе в личный кабинет – логина и пароля.

16. Для обеспечения защиты от несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, МФО применяет автоматическую проверку правильности указания заемщиком логина и пароля при входе в личный кабинет.
17. Логином в системе интернет - ресурса www.aqsha.smartolet.kz является номер мобильного телефона, который заемщик указывает при прохождении процедуры Регистрации.
18. Заемщик в процессе его идентификация и аутентификации: а) указывает номер

мобильного телефона, являющегося Логином, б) вводит пароль, содержащийся в SMS - сообщении, высланный МФО на данный номер.

19. Если компьютер или мобильный телефон после входа заемщиком в личный кабинет остается бездействующим более 10 (десять) минут, осуществляется автоматический выход из личного кабинета и завершение сессии.
20. В целях безопасности сохранение логина и пароля заемщика для упрощения процедуры входа в личный кабинет не предусматривается.
21. МФО вправе в одностороннем порядке осуществлять мероприятия в сторону улучшения для заемщика, касающиеся усиления процедур безопасности от мошеннических действия, разглашения конфиденциальной информации, или иных противоправных действий в рамках выявления и предотвращения потенциальных угроз и рисков информационной безопасности.
22. МФО обеспечивает безопасное хранение электронных сообщений и иных документов, предоставленных заемщику и полученных от него, с соблюдением их целостности и конфиденциальности в течение не менее 5 (пяти) лет после прекращения обязательств сторон по договору о предоставлении микрокредита. Хранение электронных сообщений и иных документов осуществляется в том формате, в котором они были сформированы, отправлены заемщику или получены от него.
23. В случае обнаружения несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, ее несанкционированного изменения, осуществления несанкционированных действий со стороны третьих лиц, МФО, незамедлительно принимает меры для устранения причин и последствий таких действий, а также в течение одного рабочего дня информирует об этом уполномоченный орган.

ГЛАВА 5. ОПИСАНИЕ ФУНКЦИОНАЛА И ТЕХНИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО РАСПОЗНАВАНИЮ УДОСТОВЕРЯЮЩИХ ДОКУМЕНТОВ

24. Программное обеспечение «Система распознавания удостоверяющих документов «VeriDoc» (СРД) представляет собой продукт для извлечения данных из документов, удостоверяющих личность, который состоит из следующих модулей:

- Подсистема автоматического детектирования документа и определения типа на изображении;
- Подсистема извлечения и распознавания текстовых данных.
- СРД распространяется в виде двух отдельных решений:

1) библиотек для встраивания в мобильные приложения (Mobile SDK), которые содержат в себе весь функционал распознавания;
2) клиент-серверное решение (Web SDK).

Однако МФО использует Web SDK.

24.10. . **Mobile SDK** предоставляется для операционных систем Android (начиная с версии 4.4, Android API 16 и выше) и iOS (начиная с версии 10). Количество транзакций и количество установок мобильного приложения с SDK не ограничены.

24.11. . **Web SDK** состоит из серверной и клиентской части. Клиентская часть состоит из JavaScript модуля, который встраивается в веб-страницу www.aqsha.smartolet.kz. Этот модуль позволяет запрашивать разрешение на использование камеры, отображать изображение с камеры, и общаться с сервером, чтобы получить результат распознавания. Серверная часть реализована в виде Docker образа, который принимает поток запросов с изображениями документа от клиентского модуля (последовательные POST запросы), распознает документы и возвращает результаты.

24.12. . СРД имеет модуль детектирования документа, который:

- находит границы документа на изображении используя алгоритмы компьютерного зрения, при условии, что границы отступают не более чем на 20% от краев изображения во внутреннюю сторону;
- толерантен к небольшим перспективным искажениям и планарным ротациям;
- толерантен к небольшим шумам и различным условиям освещенности (не менее 300 люкс);
- автоматически производит необходимые трансформации для удаления перспективных и планарных искажений, и приводит к нормальному виду (ортогонально сверху вниз). Т.е. в случае некорректного расположения документа по направляющим (смещение картинки), модуль самостоятельно произведет выравнивание и нормализацию изображения;
- определяет тип документа на изображении с помощью алгоритмов сравнения шаблонов.

24.13. СРД имеет модуль извлечения и распознавания текстовых данных, который:
- извлекает текстовые данные из документа в зависимости от его типа;
- распознает машинописный текст из MRZ зон удостоверений личности граждан Республики Казахстан и других документов, которые соответствуют стандартам MRZ TD1, MRZ TD2 и MRZ TD3.

25. **Технические характеристики**:

Mobile SDK для интеграции в приложение:

- Размер библиотеки 6 МБ и 10 МБ для одной архитектуры процессора для Android и iOS соответственно;
- Процент ошибок распознавания удостоверяющих документов по изображениям не более 5% от общего количества транзакций.

Web SDK клиент-серверное решение:

- Данные с сервера, где работает ПО, не передаются на внешние ресурсы и серверы;
- Запросы на сервер проходят только по протоколу HTTPS;
- Клиентский JavaScript модуль поддерживает браузеры Chrome, Mozilla Firefox, Safari (на устройствах Apple только этот браузер), и другие с такими же движками.
- Рекомендуемая характеристика серверной машины: 4 x Intel CPU, RAM: 4 GB, SSD: 40 GB, доступ к интернету с высокой скоростью;

Требования к качеству предоставляемых данных:

- Необходимое разрешение изображения - 1280x720 пикселей, не замутненное;
- Изображение не должно содержать бликов от искусственного и естественного источников освещения на документе;
- Все необходимые символы должны присутствовать на изображении и быть разборчивыми;
- Распознавание проводить в хорошо и равномерно освещенном помещении;
- Минимальные требования по освещенности - 300 люкс.

Требования к камере устройства:

- Наличие функции автоматической фокусировки изображения.

26. **Описание функционала и техническая характеристика программного обеспечения по определению живости пользователя**

Модуль определения активной живости

Программное обеспечение "Система определения живости VeriLive" представляет собой ПО для детектирования живого пользователя, которое состоит из модуля предотвращения фото атаки. Система определяет является ли личность перед камерой человеком или это фотография

с дисплея или распечатка. Система просит пользователя выполнить ряд действий, указанных на экране. Например, выполнить поворот головы в указанном направлении.
С помощью глубинных нейросетей и ряда сложных алгоритмов компьютерного зрения система определяет координаты расположения глаз, рта и носа на изображениях с камеры. Набор действий, необходимый для выполнения пользователем, сложно воспроизводим для атак с экранов телефонов и распечатанных фотографий. Для дополнительной безопасности в модуль включена нейросеть, которая анализирует изображения на предмет атрибутов атаки (блики поверх лица, грани телефонов и пальцев рук, засветы и т.д.).
Максимальная точность детектирования достигается при следующих технических характеристиках:

- Камера для съемки субъекта: Фронтальная камера мобильного устройства, веб камера;
- Разрешение камеры: от 2Мпикс;
- Освещение: 200-400 люкс, без вспышки;
- В кадре только 1 лицо;
- Движение в кадре минимальное, как устройством, так и пользователем;
- Требования к телефону: Android 5.1 и выше, NDK 21, - arm-v7a, arm64-v8a, x86, x86-64; iOS 10 и выше, arm64, x86_64;
- При съемке на мобильном устройстве, держать телефон максимально ровно. Отклонения по углу не более 10 градусов;
- Функционал невозможен для использования людьми с ограниченными возможностями движения головы.

27. Описание функционала и техническая характеристика программного обеспечения по распознаванию лиц

Программное обеспечение "Система распознавания лиц «VeriFace»" (СРЛ) представляет собой ПО для распознавания лиц, которое состоит из следующих модулей: 1) модуль детектирования лица на изображении, 2) модуль выделения уникального дескриптора лица, 3) модуль сравнения лиц 1 к 1.
СРЛ имеет возможность встроиться в Мобильное приложение (SDK) как инструмент для нахождения лица, его обрезки и отправки его на сервер для получения дескриптора и сравнения. СРЛ должна работать как Серверное решение на базе Unix в качестве ПО или модуля для других ПО.
Функциональные характеристики СРЛ:
- Модуль детектирования лица на изображении:

- С помощью глубинной сверточной нейросети и ряда математических преобразований находит точное положения лица и его размер на изображении;
- В случае нахождения нескольких лиц на изображении отправляет на обработку самое большое (ближе всего находящиеся к объективу).

- Модуль выделения уникального дескриптора лица:

- производит математические вычисления на изображении, содержащем лицо человека, с помощью глубокой искусственной нейронной сети и, как результат, выделяет уникальный дескриптор лица;
- работает с лицами людей разной расовой принадлежности - монголоидная и европеоидная расы, в основном населяющих территорию РК (тюркские, среднеазиатские, славянские и западноевропейские);

● толерантен к различным уровням освещенности помещения, но не менее 200 люкс. Нежелательно использование яркой вспышки при фотографировании лица.

- Модуль сравнения лиц 1 к 1:

● производит сравнение лиц при помощи математических вычислений на основании выделенных уникальных дескрипторов изображений;

● результат сравнения лиц при помощи математических преобразований выводит в процентном выражении;

● тесно интегрирован с модулем выделения дескриптора.

Технические характеристики СРЛ:

1. Максимальная точность распознавания должна составлять 95% при соблюдении необходимых условий эксплуатации, указанных ниже:

1.1. Освещение помещения от 300 люкс;

1.2. Качество предоставляемого изображения 250 пикселей на метр;

1.3. Лицо занимает 80% изображения;

1.4. Сравниваемые изображения цветные;

1.5. Глубина цвета сравниваемых изображений 24 bit;

2. Максимальное время обработки 0,15 сек, не считая времени на отправку и получение данных;

3. Не более 100 запросов единовременно на один экземпляр системы (system instance);

4. Android 5.0 и выше (Android API 21 и выше), iOS 10 и выше.

Дополнительные функциональные характеристики СРЖ:

- Модуль по выбору лучшего кадра из видео:

● С помощью глубинной сверточной нейросети и ряда математических преобразований определяет и возвращает "лучшее" изображения пользователя из видеосессии;

● Характеристики изображения определяются такими параметрами как поворот головы пользователя, уровень белого шума, размытость и освещение.

- Модуль записи процесса определения живости:

● Запись видеосессии пользователя производится для целей архивации и последующего анализа, в случае необходимости;

● Конфигурационные настройки позволяют указать качество видео (битрейт) в диапазоне 25-2500 Кбит/сек. Данный параметр напрямую влияет на размер получаемого видеофайла.

- Модуль защиты от атак с подменой видео:

● Защита от подмены видеопотока с камеры устройства при помощи аппаратного обеспечения для атак с предварительно записанными видеосессиями пользователя;

● Защита от подмены видеопотока с камеры устройства при помощи программного обеспечения для атак с предварительно записанными видеосессиями пользователя.

ГЛАВА 6. БЕЗОПАСНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ И ИНЫХ ДОКУМЕНТОВ

28. В целях обеспечения информационной безопасности МФО выполняются следующие условия:

- по организации системы управления информационной безопасностью;
- по организации доступа к информационным активам;
- по обеспечению безопасности информационной инфраструктуры;
- по осуществлению мониторинга деятельности по обеспечению информационной

безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

- по проведению анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;
- по средствам криптографической защиты информации;
- по обеспечению информационной безопасности при доступе третьих лиц к информационным активам;
- по проведению внутренних проверок состояния информационной безопасности;
- по процессам системы управления информационной безопасностью.

29. Подлежащая защите информация может:

- размещаться на бумажных носителях;
- существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);
- передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
- присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.
- Требования к обеспечению информационной безопасности при организации деятельности МФО в части договоров на предоставление сведений о потенциальных заемщиках (данные об официальных доходах, перечислениях из ГФСС, о количестве и средней сумме пенсионных выплат из республиканского бюджета, данных кредитного отчета и другие отчеты) от ТОО «Первое кредитное бюро» (далее – ПКБ) в рамках заключенных договоров**:**

31.1. МФО обеспечивает конфиденциальность и целостность информации, получаемой из информационной системы ПКБ.

31.2. МФО обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями Договоров, заключенных с ПКБ.

31.3. МФО обеспечивает исполнение организационно-технических, технологических требований и мер, необходимых для функционирования и защиты системного и прикладного программного обеспечения, используемого для взаимодействия с информационной системой ПКБ и обработки получаемой из нее информации.

31.4. При использовании оборудования для работы с информационной системой ПКБ учитывается необходимость его защиты от несанкционированного доступа, а также защиты носителей информации и сетевых ресурсов, используемых для работы с информационной системой ПКБ.

31.5. МФО определяет и утверждает перечень ответственных лиц.

31.6. МФО обеспечивает наличие подписанных ответственными (ответственным) лицами (лицом) организации обязательств о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими функциональных обязанностей.

31.7. МФО обеспечивает наличие внутренних документов, определяющих порядок определения и утверждения перечня ответственных лиц, их права и ответственность (включая должностные инструкции).

31.8. Доступ к информации предоставляется работникам МФО в объеме, необходимом для исполнения их функциональных обязанностей.

31.9. Учетная запись ответственного лица, по которой он идентифицируется в информационной системе ПКБ, соответствует конкретному физическому лицу.

31.10. МФО по запросу уполномоченного органа представляет сведения, подтверждающие его соответствие требованиям, предусмотренным в договорах с ПКБ.

31.11. Операционная система рабочей станции обеспечивает функции идентификации и аутентификации пользователя, а также разграничения прав доступа пользователей и авторизации в соответствии с назначенными правами.

31.12. МФО использует собственную рабочую станцию.

31.13. При использовании рабочей станции для подключения к информационной системе Кредитного бюро одновременное подключение к другим ресурсам сети интернет не производится.

31.14. Работники МФО обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.

31.15. Работники МФО обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы Кредитного бюро.

31.16. Ответственность за обеспечение информационной безопасности МФО возлагается на все структурные подразделения МФО в рамках их полномочий и в соответствии с положениями, установленными настоящими Процедурами и разработанными на ее основе документами.

32. За нарушение требований настоящих Процедур и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами МФО и законодательством РК.

ГЛАВА 7. МЕРЫ ПРОФИЛАКТИКИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

33. В профилактике инцидентов кибербезопасности важную роль играет соблюдение соответствующих национальных и международных требований при разработке программного обеспечения, проектировании компонентов информационных систем и инфраструктуры финансового сектора. МФО выполняет регулярную оценку рисков кибербезопасности, которая служит основой для выработки и применения мер по минимизации данных рисков, а также оценки эффективности реализованных мер.

34. Учитываются результаты, полученные на этапе профилактики (предотвращения), а также опыт уже обработанных инцидентов. Своевременно оценивается характер, масштабы и последствия инцидентов кибербезопасности, в целях снижения результатов их воздействия, своевременно уведомляются внутренние и внешние заинтересованные стороны и координируются совместные действия по реагированию. К заинтересованным сторонам относятся:

- Национальный Банк Республики Казахстан;
- иные уполномоченные государственные и законодательные органы, осуществляющие регулирование деятельности МФО;
- заемщики;
- кредиторы и инвесторы;
- работники структурных подразделений, осуществляющие взаимодействие в процессе осуществления деятельности МФО;
- поставщики услуг.

35. Обеспечивается продолжение операционной деятельности после инцидента при одновременном выполнении процедур восстановления, в том числе:

- устранения последствий инцидента;
- восстановления нормального состояния информационных систем и данных с подтверждением их нормального состояния;
- выявления и устранения уязвимостей, которые были использованы в рамках инцидента, в целях недопущения подобных инцидентов в будущем;
- обеспечения надлежащего информационного обмена внутри страны и за ее пределами.

36. Повышение информированности и компетенции, как пользователей, так и работников (повышение квалификации, обучение) помогут устранить риски и создать культуру безопасного создания и использования информации в МФО. На этапе повышения

осведомленности следует использовать опыт, полученный в ходе профилактики и реагирования, чтобы пользователи были ознакомлены с реальными рисками и эффективными методами их минимизации.

37. В случае обнаружения несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, ее несанкционированного изменения, осуществления несанкционированных действий со стороны третьих лиц, МФО незамедлительно принимает меры для устранения причин и последствий таких действий, а также в течение одного рабочего дня информирует об этом уполномоченный орган.

38. МФО принимает меры по предотвращению использования действующих или внедряемых способов и технологий предоставления микрокредитов электронным способом в схемах легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма. При предоставлении микрокредитов и проведении кредитного скорринга потенциального заемщика МФО применяет необходимые меры, предусмотренные Законом Республики Казахстан от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон о ПОДФТ), а также в соответствии с Постановлением Правления Национального Банка Республики Казахстан О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 25 декабря 2013 года № 292 "О введении ограничений на проведение отдельных видов банковских и других операций финансовыми организациями".

ГЛАВА 8. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В НАСТОЯЩИЕ ПРОЦЕДУРЫ

39. Предложения о внесении изменений и дополнений в настоящие Процедуры могут быть инициированы любым сотрудником МФО посредством предоставления их в письменном виде директору МФО.
40. Внесение изменений и дополнений в настоящие Процедуры производятся в соответствии с изменениями в Законодательстве Республики Казахстан и при необходимости.