Общество с ограниченной ответственностью

«Микрокредитная компания «Ахтан»

Утверждаю

Директор _____ Ахтариев А.Х.

«___»_____2019 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

г. Октябрьский

2019 г.

1. Перечень используемых определений, обозначений и сокращений.

АИБ — Администратор информационной безопасности.

ИБ — Информационная безопасность.

ИР — Информационные ресурсы.

ИС — Информационная система.

НСД — Несанкционированный доступ.

СЗИ — Средство защиты информации.

СУИБ — Система управления информационной безопасностью.

ЭВМ — Электронная — вычислительная машина, персональный компьютер.

Администратор информационной безопасности — специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации — возможность получения информации и ее использования.

Идентификация — присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация — это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность — механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т. п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система — совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач в Обществе с ограниченной ответственностью «Микрокредитная компания «Ахтан» (далее — «Общество»).

Информационные ресурсы — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Конфиденциальность — доступ к информации только авторизованных пользователей.

Несанкционированный доступ к информации — доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности — комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Общество для обеспечения его информационной безопасности.

Регистрационная (учетная) запись пользователя — включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т. п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т. п. Она также может содержать такие сведения о пользователе, как Ф. И. О., название подразделения, телефон и т. п.

Угрозы информации — потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и

хранения данных, т. е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость — недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.

2. Вводные положения.

2.1 Введение.

Политика информационной безопасности Общества определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми в последствии руководствуется в своей деятельности.

2.2 Цели.

Основными целями Политики информационной безопасности являются защита информации Общества от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а так же обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности.

Общее руководство обеспечением ИБ осуществляется Директором Общества.

Сотрудники Общества обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов Общества по вопросам обеспечения ИБ.

2.3 Задачи.

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба Обществу обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Общества), либо иметь непреднамеренный ошибочный характер.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание организации СУИБ;

определение порядка сопровождения ИС в Обществе.

3. Политика информационной безопасности Общества.

3.1 Назначение Политики информационной безопасности.

Политика информационной безопасности Общества — это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Обществе.

Политика информационной безопасности относятся к административным мерам обеспечения ИБ и определяют стратегию Общества в области ИБ.

Политика информационной безопасности регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика ИБ реализуется

посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

3.2 Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

- постоянный и всесторонний анализ информационного пространства Общества с целью выявления уязвимостей информационных активов;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ Общества, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Общества, а также повышать трудоемкость технологических процессов обработки информации;
- контроль эффективности принимаемых защитных мер;
- персонификация и адекватное разделение ролей и ответственности между сотрудниками Общества, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3 Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе.

Обучение сотрудников Общества в области ИБ проводится согласно плану, утвержденному Директором Общества.

Допуск персонала к работе с защищаемыми ИР Общества осуществляется только после его ознакомления с настоящей Политикой.

3.4 Учетные записи.

Настоящая Политика определяет основные правила присвоения учетных записей пользователям информационных активов Общества. Регистрационные учетные записи подразделяются на:

-пользовательские — предназначенные для идентификации/аутентификации пользователей информационных активов Общества;
-системные — используемые для нужд операционной системы;
-служебные — предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Общества назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

3.5 Защита автоматизированного рабочего места.

Настоящая Политика определяет основные правила и требования по защите информации Общества от неавторизованного доступа, утраты или модификации.

Положения данной Политики определяются в соответствии с используемым техническим решением.

4. Профилактика нарушений Политики информационной безопасности.

Под профилактикой нарушений Политики информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Обществе и проведение разъяснительной работы по ИБ среди пользователей.

4.1 Ликвидация последствий нарушения Политики информационной безопасности.

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР, ИС рекомендуется уведомить Директора, и далее следовать указаниям.

4.2 Ответственность за нарушение Политики информационной безопасности.

Ответственность за выполнение правил Политики информационной безопасности несет каждый сотрудник Общества в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики информационной безопасности Общества, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Лист ознакомления

№	ФИО и должность Работника	Дата ознакомления	Подпись