ООО МКК «КРК-ФИНАНС»

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ общества с ограниченной ответственностью микрокредитная компания «КРК-Финанс»

(утверждена и введена в действие приказом
директора ООО МКК «КРК-Финанс» от 25 декабря 2018 года)

В редакции №1 от 25.12.2018

Содержание

1. Общие положения

1.1. Настоящая Политика информационной безопасности(далее – Политика) ООО МКК «КРК-Финанс» разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности согласно с требованиями федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается в том числе на:

- Доктрине информационной безопасности Российской Федерации;
- Федеральном законе от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- Федеральном законе от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации».

1.2. Настоящая Политика является открытым документом, доступным любому сотруднику ООО МКК «КРК-Финанс»(далее – Организация) и клиенту организации, представляет собой официально принятую руководством Организации систему взглядов на проблему обеспечения информацонной безопасности и устанавливает принципы построения системы управления информационной безопасностью.

1.3. Необходимые требования обеспечения информацонной безопасности должны неукоснительно соблюдаться сотрудниками Организации и другими сторонами как это определяется положениями внутренних нормативных документов Организации, а так же требованиями договоров и соглашений, стороной которых является Организация.

1.4. Настоящая Политика является документом по информационной безопасности первого уровня.

1.5. Настоящая Политика распространяется на бизнес-процессы Организации и обязательна для применения всеми сотрудниками и руководством Организации, а так же пользователями информационных ресурсов Организации.

1.5. Документами, детализирующими положения настоящей Политики, являются частные политики обеспечения информационной безопасности, которые являются документами по информационной безопасности второго уровня. Частные политики обеспечения информационной безопасности оформляются как отдельные внутренние документы Организации, разрабатываются и согласовываются в соответствии с установленным в Организации порядком и утверждаются лицом, ответственным в вопросах информационной безопасности Организации.

2. Список терминов и определений

№ п/п	Термин	Определение термина
1.	**Организация**	Общество с ограниченной ответственностью микрокредитная компания «КРК-Финанс»
2.	**Бизнес-процесс**	Последовательность технологически связанных операций по предоставлению кредитных продуктов и/или осуществлению конкретного вида обеспечивающей деятельности Организации.
3.	**Пользователь информационной системы**	Физическое лицо, обладающее возможностью доступа к информационной системе Организации.
4.	**Информационная система Организации**	Совокупность программно-аппаратных комплексов Организации, применяемых для обеспечения производственных процессов Организации.
5.	**Информационная безопасность Организации**	В настоящей Политике под этим понимается состояние защищённости технологических, организационных и производственных процессов Организации, объединяющих в своём составе сотрудников Организации, технические и программные средства обработки информации, информацию в условиях угроз в информационной среде.
6.	**Рисковое событие информационной безопасности**	Событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Организации и произошедшее по причине ошибочности или сбоя процессов Организации, действий людей и систем, а так же по причине внешний событий.
7.	**Угроза информационной безопасности**	Операционный риск, влияющий на нарушение одного или нескольких свойств информации – целостности, конфиденциальности, доступности объектов защиты.
8.	**Модель угроз**	Описательное представление свойств или характеристик угроз безопасности информации.

9.	**Модель нарушителя**	Описательное представление опыта, знаний, доступных ресурсов возможных нарушителей информационной безопасности Организации, необходимых им для реализации угрозы информационной безопасности, и возможной мотивации действий.
10.	**Инцидент информационной безопасности**	Появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которым связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры, и создания угрозы информационной безопасности.

3**. Описание объекта защиты**

Основными объектами защиты системы информационной безопасности в Организации являются:

- информационные ресурсы, содержащие коммерческую тайну, персональные данные сотрудников и клиентов Организации, сведения ограниченного распространения, а так же открыто распространяемую информацию, необходимую для работы Организации, независимо от формы и вида его представления;

- информационные ресурсы, содержащие конфиденциальную информацию, сведения ограниченного распространения, а так же открыто распространяемую информацию, необходимую для работы Организации, независимо от формы и вида его представления;

- информационная инфраструктура, включающая в себя системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размешены такие системы;

- сотрудники Организации, использующие или управляющие информационно-телекоммуникационными системами Организации и их отдельными элементами;

- сведения о порядке действий сотрудников Организаций при возникновении внештатных ситуаций.

4. **Цели и задачи деятельности по обеспечению информационной безопасности**

Целью деятельности по обеспечению информационной безопасности Организации является снижение угроз информационной безопасности до приемлемого для Организации уровня.

Основные задачи деятельности по обеспечению информационной безопасности Организации:

- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- предотвращение инцидентов информационной безопасности;
- исключение, либо минимизация выявленных угроз;
- обучение, контроль знаний сотрудников Организации по вопросам информационной безопасности;
- эффективное управление рисками информационной безопасности.

5. **Угрозы информационной безопасности**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные.

5.1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей. К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Организации и контрольных органов сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

5.2. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

5.3. Возникновение естественных угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера,

стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре Организации могут быть как внешними, так и внутренними.

6. **Модель нарушителя информационной безопасности**

По отношению к Организации нарушители могут быть разделены на внешних и внутренних нарушителей.

6.1. Внутренние нарушители. В качестве потенциальных внутренних нарушителей Организацией рассматриваются:

- зарегистрированные пользователи информационных систем Организации;
- сотрудники Организации, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Организации, но имеющие доступ в здания и помещения;
- сотрудники самостоятельных структурных подразделений Организации, задействованные в сопровождении и программного обеспечения;
- руководители различных уровней.

6.2. Внешние нарушители. В качестве потенциальных внешних нарушителей Организацией рассматриваются:

- бывшие сотрудники Организации;
- представители организаций, взаимодействующих по вопросам технического и иного обеспечения Организации;
- клиенты Организации;
- посетители помещений Организации;
- конкурирующие с Организацией кредитные организации;
- члены преступных организаций или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в информационные системы Организации из внешних телекоммуникационных сетей.

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия;

- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии, и другие средства и методы для достижения стоящих перед ним целей;
- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

7. **Основные положения по обеспечению информационной безопасности**

7.1. Требования об обеспечении информационной безопасности Организации обязательны к соблюдению всеми сотрудниками Организации и пользователями информационных систем.

7.2. Руководители структурных подразделений(отделов, филиалов) Организации ответственны за обеспечение выполнения требований Политики в своих подразделениях.

7.3. Неисполнение или некачественное исполнение сотрудниками Организации и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а так же применение к виновным административных мер воздействия, степень которых определяетсмя установленным в Организации порядком либо требованиями действующего законодательства.

7.4. При планировании мероприятий по обеспечению информационной безопасности в Организации осуществляются:

7.4.1. Определение и распределение ролей сотрудников Организации, связанных с обеспечением информационной безопасности(ролей информационной безопасности).

7.4.2. Оценка важности информационных активов с учётом потребности в обеспечении их свойств с точки зрения информационной безопасности;

7.4.3. Менеджмент рисков информационной безопасности, включающий:

- анализ влияния на информационную безопасность Организации применяемых в деятельности Организации технологий, а также внешних по отношению к Организации событий;

- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз информационной безопасности;
- выявление, анализ и оценка значимых для Организации угроз информационной безопасности;
- выявление возможных негативных последствий для Организации, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Организации;
- идентификацию и анализ рисковых событий информационной безопасности;
- оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Организации;
- обработку результатов оценки рисков информационной безопасности;
- оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Организации в случае наступления рисковых событий;
- оценку влияния защитных мер на цели основной деятельности Организации;
- оценку затрат на реализацию защитных мер;
- рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Организации и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
- документальное оформление целей и задач обеспечения информационной безопасности Организации и актуализация нормативного обеспечения деятельности в сфере информационной безопасности.

7.5. Менеджмент инцидентов информационной безопасности, включающий:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;

- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Организации информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
- повышение уровня знаний сотрудников Организации в вопросах обеспечения информационной безопасности;
- контроль деятельности сотрудников и других пользователей информационных систем Организации, направленный на выявление и предотвращение конфликтов интересов;
- контроль реализации и исполнения сотрудниками Организации
- обеспечение регламентации требований действующих внутренних нормативных документов по обеспечению информационной безопасности Организации;
- и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Банка и информации, обрабатываемой в них;
- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения Организации, исключающий возможность бесконтрольного доступа в здания и помещения Организации с помощью специальных средств охраны, видеонаблюдения, оповещения.

7.6. В целях совершенствования деятельности по обеспечению информационной безопасности в Организации осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Организации).

8. **Контроль за соблюдением положений Политики**

Общий контроль состояния информационной безопасности Организации осуществляет Директор ООО МКК «КРК-Финанс».

Текущий контроль соблюдения настоящей Политики осуществляет <??ИТ-отдел>. Контроль осуществляется путём проведения мониторинга и менеджмента инцидентов информационной безопасности Организации, по результатам оценки информационной безопасности, а так же в рамках иных контрольных мероприятий.

9. **Ответственность за соблюдение положений Политики**

Общее руководство обеспечением информационной безопасности Организации осуществляет IT-специалист.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Организации лежат на IT-специалисте.

10. **Заключительные положения**

10.1. Требования настоящей Политики могут развиваться другими внутренними нормативными документами Организации, которые дополняют и уточняют её.

10.2. В случае изменения действующего законодательства и иных нормативных актов, а так же Устава Организации, настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а так же Уставу Организации. В этом случае IT-специалист обязан незамедлительно инициировать внесение соответствующих изменений.

10.3. Ответственным за внесение изменений в настоящую Политику является IT-специалист.