Микро Лизинг

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИООО "МИКРО ЛИЗИНГ"

Версия 2.0

Гомель, 2022 год

Оглавление

Иностранное общество с
ограниченной ответственностью
«Микро Лизинг»

УТВЕРЖДАЮ
Директор Иностранного
общества с ограниченной
ответственностью
«Микро Лизинг»

_____ /Н.Д. Чеботарь/
«01» декабря 2022 г.

Редакция от 16.01.2023

ПОЛИТИКА
информационной безопасности
ИООО "Микро Лизинг"

1. Введение

1.1. Настоящая Политика информационной безопасности ИООО «Микро Лизинг» (далее – Политика) определяет систему взглядов на цели и задачи в области информационной безопасности, а также общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИООО «Микро Лизинг» (далее – Организация).

1.2. Политика разработана в соответствии с действующим законодательством Республики Беларусь по вопросам защиты информации.

1.3. Политика представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных и технических аспектов обеспечения информационной безопасности (далее – ИБ) в Организации при осуществлении коммерческой деятельности.

1.4. Политика является документом по ИБ верхнего уровня, основой для формирования и проведения в Организации единой политики в области информационной безопасности, а также для принятия управленческих решений и разработки практических мер по ее применению.

1.5. Документами нижнего уровня по ИБ, детализирующими положения Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Организации, являются регламенты по обеспечению ИБ, которые оформляются как отдельные локальные правовые акты, разрабатываются, согласовываются, и утверждаются в соответствии с установленным в Организации порядком.

1.6. Обеспечение ИБ является неотъемлемой частью деятельности Организации.

1.7. Для целей настоящей Политики к сотрудникам Организации приравниваются физические лица, выполняющие работы/оказывающие услуги в пользу Организации по договорам гражданско-правового характера (если иное не вытекает из существа отношений или требований законодательства).

2. Термины и определения

2.1. Для целей данной Политики применяются термины и их определения в

значениях, определенных Законом Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации», а также следующие термины и их определения:

актив – материальный или нематериальный ресурс, представляющий ценность для Организации;

бизнес-процесс – последовательность технологически связанных операций по предоставлению услуг и/или осуществлению конкретного вида основной деятельности Организации;

информационная безопасность (ИБ) – состояние защищенности технологических и бизнес-процессов Организации, объединяющих в своем составе сотрудников Организации, технические и программные средства обработки информации, в том числе программные средства привлеченные по договору сотрудничества, информацию в условиях угроз в информационной сфере;

информационная система (ИС) – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

инцидент информационной безопасности – это появление одного или ряда нежелательных и (или) непредвиденных событий в области ИБ, при которых имеется значительная вероятность компрометации бизнес-процессов и угрозы ИБ;

пользователь информационной системы – сотрудник Организации (и/или лица выполняющие работы (оказывающие услуги) по гражданско-правовым договорам), обладающий возможностью доступа к информационной системе Организации;

событие информационной безопасности – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или отказ средств защиты, а также возникновение ранее неизвестной ситуации, которая может быть связана с ИБ.

3. Цели и задачи деятельности по обеспечению ИБ Организации

3.1. В Организации создается и функционирует система ИБ.

3.2. Главной целью системы ИБ Организации является снижение угроз до уровня, который соответствует стандартам, определенным согласно законодательству Республики Беларусь, устойчивое функционирование, защита законных интересов Организации, клиентов и контрагентов.

3.3. Целями системы ИБ Организации являются:

1) Сохранение целостности, конфиденциальности, доступности, сохранности и подлинности информационных ресурсов, эксплуатируемых Организацией информационных систем;

2) Обеспечение непрерывности доступа к информационным ресурсам Организации для поддержания функционирования процессов;

3) Защита информации от внутренних и внешних угроз с целью поддержания возможностей ведения основной деятельности Организации и принятия эффективных управленческих решений;

4) Повышение осведомленности пользователей информационных систем Организации в области рисков ИБ, связанных с информационными системами и ресурсами Организации;

5) Определение степени ответственности и обязанностей сотрудников по

обеспечению ИБ Организации.

3.4. Для обеспечения достижения целей информационной безопасности в Организации функционирует режим защиты информации, находящейся в информационных системах, используемых Организацией.

3.5. Режим защиты информации устанавливается для следующей информации:

– находящейся в информационных системах, эксплуатируемых Организацией;

– составляющей коммерческую тайну Организации и ее контрагентов при ведении основной деятельности Организации;

– которая передается третьим лицам в связи с функционированием ИС Организации.

3.6. Основными объектами защиты системы ИБ в Организации являются:

– информационные системы, эксплуатируемые Организацией. Перечень информационных систем Организации, отнесенных к соответствующим классам типовых информационных систем представлен в Приложении 1;

– информационные ресурсы, содержащие коммерческую и иную тайну Организации и ее контрагентов;

– персональные данные физических лиц;

– открыто распространяемая информация, необходимая для осуществления бизнес-процессов Организации, независимо от формы и вида ее представления;

– информационная инфраструктура, включающая системы обработки информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

4. Цели и принципы защиты информации

4.1. Защите подлежит информация, неправомерное действие в отношении которой может причинить вред ее обладателю, пользователю или иному лицу.

4.2. Целями защиты информации являются:

1) обеспечение непрерывности ведения основной деятельности Организации;

2) недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий;

3) обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

4.3. Принципами защиты информации Организации являются:

1) простота использования информационной системы и ее средств защиты информации – простота использования ИС является необходимым условием для снижения числа ошибочных действий. При этом данный принцип информационной безопасности не означает простоту архитектуры и снижение

функциональности ИС;

2) контроль над операциями в ИС – непрерывный контроль состояния ИБ и всех событий, влияющих на ИБ, в том числе автоматизированный контроль действий, совершенных пользователем и их последующий анализ;

3) запрещено всё, что не разрешено – доступ ко всем объектам ИС предоставляется только при наличии соответствующего правила. При этом основной функцией системы ИБ является разрешение, а не запрещение каких-либо действий;

4) открытая архитектура ИС – безопасность не обеспечивается через неясность;

5) разграничение доступа – каждому пользователю предоставляется доступ к информации и ее носителям в соответствии с его полномочиями. При этом исключена возможность превышения полномочий. Каждой роли/должности/группе пользователей можно назначить свои права на выполнение действий (чтение/изменение/удаление) над определенными объектами ИС;

6) минимальные привилегии – заключается в выделении пользователю наименьших прав и доступа к минимуму необходимых функциональных возможностей программ;

7) принцип равнозначности действий, совершенных от имени пользователя (с использованием учетных данных пользователя) действиям, совершенным самим пользователем;

8) достаточная стойкость – принцип выражается в том, что потенциальные злоумышленники должны встречать препятствия в виде достаточно сложных вычислительных задач.

5. Основные положения по обеспечению ИБ

5.1. Стратегия Организации в части противодействия угрозам ИБ заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности от организационных мер на уровне руководства Организации до специализированных мер ИБ по каждому выявленному в Организации риску, основанных на оценке рисков ИБ.

5.2. С целью поддержки заданного уровня защищенности, Организация придерживается процессного подхода в построении системы защиты информации.

5.3. ИБ Организации основывается на осуществлении основных процессов, соответствующих требованиям стандартов по обеспечению ИБ.

5.4. На всех этапах жизненного цикла, управление информационной безопасностью Организации осуществляется с соблюдением локальных правовых актов, определяющих процессы управления рисками в Организации.

5.5. При планировании мероприятий по обеспечению ИБ в Организации осуществляются:

1) определение и распределение ролей сотрудников Организации, связанных с обеспечением ИБ (ролей ИБ);

2) оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения ИБ;

3) управление рисками ИБ, включающее:

– анализ влияния на ИБ применяемых в деятельности Организации технологий, а также внешних по отношению к Организации событий;

– выявление проблем обеспечения ИБ, анализ причин их возникновения, прогнозирование их развития и способы их оперативного устранения;

– выявление, анализ и оценка значимых для Организации угроз ИБ;

– выявление возможных негативных последствий для Организации, наступающих в результате проявления факторов риска ИБ, в том числе связанных с нарушением свойств безопасности информационных активов Организации;

– идентификация и анализ рисковых событий ИБ;

– оптимизация рисков ИБ за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Организации в случае наступления рисковых событий;

– оценка влияния защитных мер на цели основной деятельности Организации;

– оценка затрат на реализацию защитных мер;

– рассмотрение и оценка различных вариантов решения задач по обеспечению ИБ;

– документальное оформление целей и задач обеспечения ИБ Организации, поддержка в актуальном состоянии локально-правового обеспечения деятельности в сфере ИБ.

5.6. В рамках реализации деятельности по обеспечению ИБ в Организации осуществляется управление инцидентами ИБ, включающее:

1) сбор информации о событиях ИБ;

2) выявление и анализ инцидентов ИБ;

3) расследование инцидентов ИБ;

4) оперативное реагирование на инциденты ИБ;

5) минимизация негативных последствий инцидентов ИБ;

6) оперативное доведение до руководства Организации информации по наиболее значимым инцидентам ИБ и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты ИБ;

7) выполнение принятых решений по всем инцидентам ИБ в установленные сроки;

8) пересмотр применяемых требований, мер и механизмов по обеспечению ИБ по результатам рассмотрения инцидентов ИБ;

9) изучение инцидентов ИБ, произошедших в иных организациях, проверка возможности возникновения данных инцидентов в Организации;

10) повышение уровня знаний сотрудников Организации в вопросах обеспечения ИБ путем обучения сотрудников, проведения тренингов по ИБ, иных мер;

11) обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Организации и информации, обрабатываемой в них;

12) применение средств защиты информации;

13) применение средств криптографической защиты информации;

14) обеспечение бесперебойной работы информационных систем;

15) обеспечение возобновления работы информационных систем после прерываний и нештатных ситуаций;

16) применение средств защиты от вредоносных программ;

17) обеспечение ИБ на стадиях жизненного цикла информационных

систем Организации, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);

18) обеспечение ИБ при использовании доступа в сеть Интернет и услуг электронной почты;

19) контроль доступа в здания и помещения Организации для сотрудников Организации и особый режим доступа для третьих лиц.

5.7. В целях проверки деятельности по обеспечению ИБ в Организации осуществляются:

1) контроль правильности реализации и эксплуатации защитных мер;

2) контроль изменений конфигурации информационных систем Организации;

3) мониторинг факторов рисков и их соответствующий пересмотр;

4) контроль реализации и исполнения требований сотрудниками Организации действующих локальных правовых и иных актов по обеспечению ИБ Организации;

5) контроль деятельности сотрудников Организации и других пользователей информационных систем Организации, направленный на выявление и предотвращение конфликтов интересов.

5.8. Информация об инцидентах ИБ, которые могут привести к сбоям, нарушению функционирования информационных систем, заносится в журнал учета инцидентов ИБ. Журнал ведется в электронном виде, форма журнала представлена в Приложении 2.

5.9. В целях совершенствования деятельности по обеспечению ИБ в Организации осуществляется периодическое, а при необходимости оперативное, уточнение (пересмотр) целей и задач обеспечения ИБ (при изменениях целей и задач основных бизнес-процессов Организации).

6. Организационная основа деятельности по обеспечению ИБ

6.1. В целях выполнения задач по обеспечению ИБ Организации, в соответствии с рекомендациями международных и национальных стандартов по ИБ в Организации определены следующие роли:

1) руководитель Организации;

2) должностное лицо, выполняющее функции по технической и (или) криптографической защите информации (далее – Ответственный сотрудник);

3) сотрудник Организации.

6.2. При необходимости, регламентами ИБ могут быть определены и другие роли по ИБ.

6.3. Оперативная деятельность и планирование деятельности по обеспечению ИБ Организации осуществляются и координируются Ответственным сотрудником.

6.4. Задачами Ответственного сотрудника являются:

1) установление потребностей Организации в применении мер обеспечения ИБ, определяемых как внутренними корпоративными требованиями, так и требованиями локальных правовых актов;

2) соблюдение действующего законодательства, нормативных правовых актов государственных органов, уполномоченных в области обеспечения ИБ, технической и криптографической защиты информации;

3) участие в разработке и пересмотре локальных правовых и иных актов по вопросам обеспечения ИБ Организации, включая планы, политики, положения, регламенты, инструкции, перечни сведений;

4) осуществление контроля актуальности и непротиворечивости локальных правовых и иных актов, затрагивающих вопросы ИБ Организации;

5) обучение, контроль и непосредственное взаимодействие с сотрудниками Организации в области обеспечения ИБ;

6) планирование применения средств обеспечения ИБ на объектах и информационных системах Организации;

7) выявление и предотвращение реализации угроз ИБ;

8) выявление и реагирование на инциденты ИБ;

9) информирование в установленном порядке руководителя Организации об угрозах и рисках ИБ;

10) прогнозирование и предотвращение инцидентов ИБ;

11) пресечение несанкционированных действий нарушителей ИБ;

12) обеспечение эксплуатации средств и механизмов обеспечения ИБ;

13) мониторинг и оценка ИБ, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению ИБ Организации;

14) контроль обеспечения ИБ Организации, в том числе и на основе информации об инцидентах ИБ, результатах мониторинга, оценки и аудита ИБ;

15) информирование руководителя Организации и руководителей структурных подразделений об угрозах ИБ, влияющих на деятельность Организации.

6.5. Ответственный сотрудник вправе создавать оперативные группы для проведения расследований инцидентов ИБ и может, при наличии обоснованной необходимости, по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников других структурных подразделений Организации на основе совмещения работы в группе с основными должностными обязанностями.

6.6. Основными функциями руководителя Организации в вопросах ИБ являются:

1) Назначение Ответственных сотрудников в области ИБ;

2) Координация и внедрение ИБ в Организации.

6.7. Основными задачами сотрудников Организации при выполнении возложенных на них обязанностей и в рамках их участия в деятельности по обеспечению ИБ Организации являются:

1) соблюдение требований ИБ, устанавливаемых нормативными правовыми и иными актами Организации;

2) выявление и предотвращение реализации угроз ИБ в пределах своей компетенции;

3) выявление и оперативное реагирование на инциденты ИБ;

4) информирование в установленном порядке Ответственных сотрудников о выявленных рисках ИБ;

5) прогнозирование и предотвращение инцидентов ИБ в пределах своей компетенции;

6) мониторинг и оценка ИБ в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;

7) оперативное информирование своего руководства и Ответственного

сотрудника о выявленных угрозах в ИС Организации.

7. Ответственность за неисполнение положений Политики

7.1. Положения Политики обязательны к соблюдению всеми сотрудниками Организации и пользователями информационных систем Организации.

7.2. В договорах с третьими лицами, получающими доступ к ИС Организации, оговаривается обязанность и размер ответственности третьего лица по соблюдению требований ИБ Организации. Указанные пункты изложены в заключаемом соглашении о неразглашении конфиденциальной информации;

7.3 На лиц, выполняющих работы/оказывающих услуги в пользу Организации по договорам гражданско-правового характера, а также лиц, командированных в Организацию, положения настоящей Политики распространяются в случае, если такое лицо имеет доступ к ИС Организации.

7.4. Неисполнение или ненадлежащее исполнение сотрудниками Организации и пользователями информационных систем обязанностей по обеспечению ИБ может повлечь лишение их доступа к информационным системам, а также применение к виновным мер воздействия, степень которых определяется в соответствии с требованиями действующего законодательства Республики Беларусь и локальных правовых актов Организации.

8. Контроль за соблюдением положений Политики

8.1. Общий контроль состояния ИБ Организации осуществляется руководителем Организации.

8.2. Текущий контроль соблюдения настоящей Политики осуществляет Ответственный сотрудник. Контроль осуществляется путем проведения мониторинга и управления инцидентами ИБ Организации, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

8.3. Ответственным сотрудником организована периодическая проверка соблюдения обеспечения ИБ с последующим представлением отчета по результатам указанной проверки руководителю Организации.

9. Порядок организации информационного взаимодействия с иными информационными системами

9.1. Порядок взаимодействия ИС с иными информационными системами определяется соответствующими документами по каждому подключению. Взаимодействие с внешними информационными системами организуется в соответствии с общей схемой системы защиты информации ИС.

9.2. Взаимодействие ИС Организации и иных информационных систем осуществляется в автоматизированном и (или) автоматическом режиме.

9.3. Функционирование ИС Организации осуществляется с синхронизацией времени с интернет-ресурсом Белорусского государственного института метрологии (БелГИМ) belgim.by и обновлением системного, прикладного программного обеспечения и антивирусных баз с соответствующих ресурсов.

9.4. Обновление баз средств антивирусной защиты информации осуществляется автоматически, на ежедневной основе.

9.5. Доступ к сети Интернет предоставляется в рамках необходимых

разрешений только авторизованным сервисам и сотрудникам Организации, которым доступ разрешен.

9.6. К авторизованным сервисам Организации относятся:

- обновление системного и прикладного ПО;
- обновление встроенного ПО технических средств;
- обновление антивирусных средств защиты информации;
- синхронизация времени с источником надежного времени.

9.7. Для взаимодействия ИС Организации с иными информационными системами должны применяться средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы.

9.8. Взаимодействие иных информационных систем с ИС Организации осуществляется путем обеспечения информационной и технологической совместимости иных информационных систем с ИС. Взаимодействие информационных систем с ИС Организации осуществляется согласно Приложению 4 "Требования к организации взаимодействия информационных систем", к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному приказом оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

9.9. Организация взаимодействия ИС Организации и иных информационных систем осуществляется на принципах соблюдения полноты, достоверности предоставляемой информации, получаемой, обрабатываемой и размещаемой в рамках межсистемного взаимодействия, а также конфиденциальности информации, доступ к которой ограничен законодательством Республики Беларусь.

10. Права и обязанности пользователей ИС

10.1. Ответственный сотрудник имеет право проводить аудиторские проверки действий сотрудников, состояния информационных ресурсов, программно-технических средств ИС. Сотрудники обязаны предоставить полный доступ к программно-техническим средствам для выполнения проверок. Замечания Ответственного сотрудника обязательны к рассмотрению. При возникновении спорных ситуаций возможна организация внешнего аудита (консультирования).

10.2. Ответственный сотрудник несет ответственность за организацию, эксплуатацию и функционирование соответствующего ПО и ресурсов ИС, включая средства защиты информации, и контроль осуществления организационно-распорядительных мер защиты.

10.3. Ответственный сотрудник несет ответственность за обеспечение следующих условий функционирования ИС на рабочих местах пользователей, имеющих доступ к ИС:

- обеспечение мер физической защиты по воспрепятствованию несанкционированному доступу к программно-техническим и сетевым средствам ИС;
- организация и контроль соблюдения сотрудниками требований Политики и локальных правовых актов по ИБ Организации, в том числе способов разграничения доступа пользователей к объектам ИС, а также порядок:

резервирования и уничтожения информации; защиты от вредоносного программного обеспечения; использования съемных носителей информации; использования электронной почты; обновления средств защиты информации; осуществления контроля (мониторинга) за функционированием информационной системы и системы защиты информации; реагирования на события информационной безопасности и ликвидации их последствий; управления криптографическими ключами, в том числе требования по их генерации, распределению, хранению, доступу к ним и их уничтожению;

– обеспечение наличия и функционирования антивирусного ПО и иных средств защиты информации.

10.4. Основные обязанности сотрудников Организации:

– до начала работы с ИС Организации сотрудники в обязательном порядке должны ознакомиться с настоящей Политикой и иными локальными правовыми актами в сфере информационной безопасности;

– знать и выполнять требования действующих нормативных документов, а также внутренних локальных правовых актов, регламентирующих порядок действий по защите информации;

– использовать ИС исключительно для выполнения должностных обязанностей;

– знать и соблюдать установленные требования по режиму обработки данных, учету, хранению и пересылке носителей информации, обеспечению безопасности, а также руководящих и организационно-распорядительных документов;

– соблюдать требования парольной политики;

– соблюдать правила при работе в сетях общего пользования и (или) международного обмена (Интернет и т.п.);

– обо всех выявленных нарушениях, связанных с ИБ, а также для получения консультаций по вопросам ИБ, обращаться к Ответственному лицу;

10.5. Сотрудникам запрещено:

– использовать программное и аппаратное обеспечение ИС в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию ИС;

– умышленно использовать недокументированные возможности и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инциденту информационной безопасности. Об обнаружении такого рода ошибок ставить в известность Ответственное лицо и руководителя своего подразделения;

– разглашать защищаемую информацию третьим лицам.

10.6. В случае нарушения требований настоящей Политики, а также при возможных иных инцидентах ИБ, сотруднику, в пределах ответственности которого произошел инцидент, может быть заблокирован доступ к ИС до окончания расследования инцидента. Сотрудник и его руководитель уведомляется о блокировании доступа. По результатам расследования материалы могут быть использованы как основание для привлечения нарушителя к дисциплинарной, административной либо уголовной ответственности в соответствии с законодательством Республики Беларусь.

11. Контроль соблюдения требований настоящего документа

11.1. Контроль за соблюдением и реализацией установленных в настоящем документе требований в процессе эксплуатации ИС Организации возлагается на руководителя Организации и руководителей структурных подразделений.

11.2. Ответственность за своевременный пересмотр настоящего документа несет Ответственный сотрудник.

11.3. Все сотрудники Организации несут персональную ответственность за нарушение требований Политики.

12. Порядок внесения изменений в настоящий документ

12.1. Для эффективного функционирования совокупности документированных правил, процедур и требований в области защиты информации, определенных в составе Политики, по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, по результатам проведения внутренних проверок по ИБ и других контрольных мероприятий, с целью обеспечения соответствия нормативным актам, предусмотрен пересмотр Политики.

12.2. Инициаторами пересмотра Политики могут выступать все сотрудники Организации в установленном порядке.

12.3. Через запланированные интервалы времени Ответственный сотрудник проводит анализ адекватности установленных правил ИБ действующим информационным процессам ИС Организации, законодательству Республики Беларусь, возможностям вычислительных ресурсов, реальным угрозам ИБ и предоставлять руководителю отчет о реальном выполнении требований и их результатах (не реже одного раза в год).

13. Заключительные положения

13.1. Требования настоящей Политики должны дополняться другими локальными правовыми и иными актами Организации.

13.2. В случае изменения действующего законодательства, локальных и иных правовых актов, а также Устава Организации Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным, локальным и иным правовым актам, а также Уставу Организации. В этом случае Ответственный сотрудник обязан инициировать внесение соответствующих изменений.

13.3. Внесение изменений в Политику осуществляется на периодической и внеплановой основе. Внеплановое внесение изменений в Политику может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.

13.4. Ответственным за внесение изменений в Политику является Ответственный сотрудник.

13.5. В развитие данной политики и конкретизацию изложенных в ней положений разработан и утвержден документ «Регламенты ИБ», который включает следующие разделы:

– порядок резервирования и уничтожения информации;
– порядок защиты от вредоносного программного обеспечения;
– порядок использования съемных носителей информации;
– порядок использования электронной почты;
– порядок обновления средств защиты информации;
– порядок осуществления контроля (мониторинга) за функционированием информационной системы и системы защиты информации;
– порядок реагирования на события информационной безопасности и ликвидации их последствий;
– порядок управления криптографическими ключами, в том числе требования по их генерации, распределению, хранению, доступу к ним и их уничтожению.

Приложение 1
к Политике информационной
безопасности ИООО «Микро Лизинг»
(в редакции от 16.01.2023)

Перечень информационных систем Организации, отнесенных к соответствующим классам типовых информационных систем

№ п.п.	Наименование ИС	Класс ИС	Ответственный за обеспечение ИБ
1	Информационная система обеспечения коммерческой деятельности иностранного общества с ограниченной ответственностью «Микро Лизинг»	3-юл, 3-ин, 3-спец	Лицо, назначенное ответственным приказом директора
2	Корпоративная электронная почта иностранного общества с ограниченной ответственностью «Микро Лизинг»	5-частн	Лицо, назначенное ответственным приказом директора