Приложение № 1
к приказу № 118 от «23» апреля 2026 г.

Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики им. А.В. Гапонова-Грехова
Российской академии наук»
(ИПФ РАН)

ПОЛИТИКА
информационной безопасности

Нижний Новгород
2026

Содержание

1. Термины, определения и сокращения 3
2. Общие положения 4
3. Цели и задачи информационной безопасности 5
4. Основные информационные активы 6
5. Основные угрозы информационным активам 6
6. Принципы обеспечения информационной безопасности 7
7. Управление рисками информационной безопасности 9
8. Основные направления обеспечения информационной безопасности 9
9. Ответственность 13
10. Заключительные положения 15
11. Нормативные документы 16

1. Термины, определения и сокращения

1.1. В настоящем документе используются следующие сокращения:

ИБ – информационная безопасность;

ИС – информационная система;

ПО – программное обеспечение;

СКЗИ – средства криптографической защиты информации;

СКУД – система контроля и управления доступом;

ФСБ России– Федеральная служба безопасности;

ФСТЭК России– Федеральная служба по техническому и экспортному контролю.

1.2. В настоящем документе используются следующие термины и определения:

- **аудит информационной безопасности –** мероприятия для проверки текущего состояния защиты информации, независимая экспертная оценка соответствия требованиям ИБ, допускающая возможность формирования профессионального аудиторского суждения о состоянии ИБ организации;
- **аутентичность** – гарантия того, что субъект, ресурс или информация идентичны заявленным;
- **достоверность** – свойство соответствия информации объективной реальности;
- **доступность** – свойство информации находиться в состоянии готовности и возможности использования по запросу авторизованного субъекта;
- **защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
- **информация** – значимые данные;
- **информационная безопасность** – обеспечение конфиденциальности, целостности и доступности информации.
- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **информационный актив** – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации, находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме (сама информация, а также вспомогательные системы и средства, используемые для защиты и надлежащей работы информационных систем организации, оборудования, носители информации и прочее);
- **инцидент информационной безопасности –** любое непредвиденное или нежелательное событие, которое может нарушить деятельность организации или информационную безопасность;

- **классификация информационных активов** – разделение существующих информационных активов по типам, выполняемое в соответствии со степенью тяжести последствий от потери активом свойств ИБ;
- **конфиденциальная информация –** информация, для которой в соответствии с законодательством Российской Федерации, нормативными документами ФСБ и ФСТЭК России и (или) внутренними документами организации обеспечивается сохранение свойства конфиденциальности;
- **конфиденциальность** – свойство информации быть недоступной или закрытой для неавторизованного индивидуума, логического объекта или процесса;
- **организация** – ИПФ РАН, включая филиалы и иные обособленные структурные подразделения;
- **пользователь** – лицо или организация, которое использует действующую информационную систему для выполнения конкретной функции;
- **работники (работники организации)** – лица, работающие в организации на основе трудового договора (контракта), с полной или частичной занятостью независимо от их должности в организации;
- **риск** – следствие влияния неопределенности на достижение поставленных целей;
- **событие информационной безопасности –** идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;
- **угроза информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
- **управление рисками информационной безопасности** – систематический процесс применения установленных процедур (оценки рисков, обработки рисков, мониторинга рисков и пересмотра рисков) к деятельности организации, связанной с использованием основных информационных активов;
- **утечка информации –** несанкционированное предоставление или распространение конфиденциальной информации, не контролируемое организацией.
- **целостность** – свойство сохранять правильность, полноту и достоверность информационных активов. Означает, что информация не была подвергнута несанкционированному изменению.

2. Общие положения

2.1. Настоящая Политика информационной безопасности (далее – Политика) разработана с целью документально определить и зафиксировать требования, правила, процедуры обеспечения информационной безопасности (далее – ИБ) в ИПФ РАН.

2.2. ИПФ РАН (далее – организация) – юридическое лицо, действующее в качестве оператора информационных систем (далее – ИС).

3. Цели и задачи информационной безопасности

3.1. Основной целью организации в области обеспечения ИБ является минимизация рисков ИБ, которым подвержены технологии и информационные системы, используемые для функционирования организации, а также обеспечение эффективности мероприятий по ликвидации неблагоприятных последствий реализации угроз и инцидентов ИБ.

3.2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;
- целостности и аутентичности информации, хранимой и обрабатываемой в ИС организации и передаваемой по каналам связи;
- доступности информации для авторизованных пользователей – устойчивого функционирования ИС организации, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время.

3.3. Достижение данной цели обеспечивается решением следующих задач:

- вовлечение руководителей и работников организации в процесс обеспечения ИБ;
- документирование требований ИБ;
- реализация мер по защите информационных активов организации от угроз ИБ;
- оптимизация стоимости владения средствами защиты информации в рамках организации;
- прогнозирование угроз и оценка рисков ИБ;
- предотвращение и/или снижение до приемлемого уровня ущерба от реализации актуальных угроз ИБ в организации;
- соблюдение законодательных, нормативных и договорных требований в области ИБ, включая требования регуляторов;
- повышение стабильности функционирования организации в условиях возможной реализации угроз ИБ;
- реагирование на инциденты ИБ;
- контроль состояния ИБ организации;
- повышение осведомленности работников организации в вопросах обеспечения ИБ;
- постоянное совершенствование систем обеспечения ИБ организации, включая проводимую политику обеспечения и управления ИБ.

4. Основные информационные активы

4.1. Основными информационными активами организации, подлежащими защите, являются:

- информация, размещенная в ИС, составляющая служебную и коммерческую тайну, персональные данные, внутренние документы ограниченного доступа, иная конфиденциальная информация, чувствительная по отношению к случайным и несанкционированным воздействиям и нарушению ее безопасности, представленная в виде электронных документов и информационных массивов, независимо от формы и вида их представления;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства обработки, передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты ИС;
- процессы обработки информации в ИС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, процессы жизненного цикла ИС.

4.2. Перечень информационных активов, подлежащих защите, определяется по результатам инвентаризации и определения ценности каждого актива с точки зрения свойств конфиденциальности, целостности и доступности.

5. Основные угрозы информационным активам

5.1. Основные угрозы информационным активам организации включают в себя:

- разглашение защищаемой информации;
- компрометацию ключевой информации, персональных идентификаторов, паролей;
- несанкционированный доступ к защищаемой информации организации;
- ввод некорректных (ложных) данных в ИС организации;
- выход из строя материальных носителей защищаемой информации;
- уничтожение (утеря) защищаемой информации;
- нештатная ситуация в работе программного обеспечения ИС организации;
- вирусное заражение;
- злонамеренные действия, осуществляемые посредством локальной вычислительной сети организации;
- целенаправленные атаки на информационные активы организации с использованием уязвимостей программного обеспечения;
- выход из строя программно-технических средств организации;
- нарушение функционирования технических мер защиты;

- несанкционированное или некорректное внесение изменений в информационные системы организации;
- несанкционированное делегирование полномочий и/или использование привилегий;
- халатность, игнорирование установленных правил обеспечения ИБ, увеличивающие вероятность реализации угрозы ИБ;
- угрозы нарушения целостности и функционирования организации в целом.

5.2. Источники угроз ИБ делятся на два основных класса:

- источники, связанные с внешними нарушителями;
- источники, связанные с внутренними нарушителями.

5.3. В качестве внешних нарушителей ИБ рассматриваются лица, не входящие в состав пользователей и обслуживающего персонала ИС организации, например, разработчики ИС, внешние лица (хакеры, члены криминальных организаций, бывшие работники организации и т.п.).

5.4. В качестве потенциальных внутренних нарушителей ИБ рассматриваются пользователи и обслуживающий персонал ИС организации, другие субъекты (лица), вовлеченные в информационные процессы организации, которые также имеют возможность санкционированного доступа к ИС и информационным активам организации.

5.5. Перечень угроз безопасности информации и нарушителей безопасности определяется в Модели угроз организации.

6. Принципы обеспечения информационной безопасности

6.1. В основе реализации обеспечения ИБ лежит комплексный подход, который включает в себя следующие группы мер защиты информации:

- организационные;
- программно-технические.

6.2. При построении ИБ организация руководствуется рядом основополагающих принципов:

6.2.1. **Неотъемлемость**

Безопасность ИС является их неотъемлемым свойством (характеристикой), а не дополнительным сервисом. Соблюдение требований ИБ обязательно для всех работников и является частью корпоративной культуры организации.

6.2.2. **Комплексность**

Согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

6.2.3. **Системность**

Обеспечение информационной безопасности организации строго и всесторонне регламентируется и является совокупностью норм, требований, положений, порядков

и инструкций, учитывающих все наиболее слабые и уязвимые места ИС и охватывающих весь их жизненный цикл.

6.2.4. **Непрерывность**

Обеспечение информационной безопасности – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС организации, начиная с самых ранних стадий их проектирования.

6.2.5. **Адекватность**

Соблюдение баланса между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками систем защиты информации.

6.2.6. **Своевременность**

Решение задач ИБ ведется одновременно с разработкой, внедрением и вводом защищаемой ИС в эксплуатацию.

6.2.7. **Упреждение**

Обеспечение ИБ акцентируется прежде всего на предотвращении (предупредительных мерах) событий ИБ, которые могут повлиять на целостность, доступность и конфиденциальность информации.

6.2.8. **Контролируемость**

Обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации, выявление и устранение уязвимостей, мониторинг событий, влияющих на состояние ИБ организации.

6.2.9. **Минимизация полномочий**

Доступ к информации предоставляется только в том случае и объеме, в каком это минимально необходимо работнику для выполнения его должностных обязанностей.

6.2.10. **Персонификация**

Все работники организации имеют персонифицированную учетную запись. Наличие учетных записей, не закрепленных за конкретным работником, не допустимо.

6.2.11. **Разрешение доступа**

Доступ к любому объекту ИС должен предоставляться только при наличии соответствующего разрешения (правила), зафиксированного в проектной документации, регламенте процесса и настройках средств защиты информации.

6.2.12. **Осведомленность**

Осведомленность работников и руководства организации в вопросах ИБ – обязательное условие безопасного функционирования систем.

6.2.13. **Персональная ответственность**

Ответственность за обеспечение безопасности информации и систем ее обработки возлагается не только на структурное подразделение по обеспечению ИБ, но и на каждого работника организации в пределах его полномочий.

6.2.14. **Вовлеченность руководства**

Осознание руководством организации необходимости обеспечения ИБ, непосредственное участие в принятии стратегических решений по вопросам функционирования системы обеспечения ИБ, включая вопросы принятия рисков.

6.2.15. **Взаимодействие и координация**

Эффективное обеспечение ИБ достигается на основе взаимодействия и координации со структурным подразделением информационных технологий, всеми заинтересованными структурными подразделениями организации, а также ФСТЭК России, ФСБ России и другими профильными министерствами, ведомствами и объединениями.

7. Управление рисками информационной безопасности

7.1. Обеспечение ИБ организации основывается на управлении рисками ИБ, что предусматривает анализ существующих угроз ИБ, оценку рисков реализации указанных угроз и принятие необходимых мер по отношению к рискам ИБ, недопустимым для организации.

7.2. Целью управления рисками ИБ является:

- минимизация негативных последствий от реализации рисков;
- оптимизация затрат, направленных на предотвращение негативных последствий от реализации рисков.

7.3. Ответственным за процесс управления рисками ИБ в организации является подразделение информационной безопасности.

8. Основные направления обеспечения информационной безопасности

8.1. **Документирование требований по ИБ**

8.1.1. В организации разрабатывается, утверждается и доводится до работников и соответствующих внешних сторон комплект документов (политик, положений, инструкций), регламентирующих отдельные направления ИБ.

8.1.2. Документы по ИБ для гарантии их постоянной пригодности, соответствия и результативности пересматриваются через запланированные интервалы времени или в случае существенных изменений процессов функционирования организации или изменений требований законодательства Российской Федерации, нормативных документов регулирующих органов.

8.2. **Организация ИБ**

8.2.1. Управление ИБ должно обеспечиваться как при осуществлении информационного обмена внутри организации, так и при взаимодействии со сторонними организациями и третьими лицами (субъектами).

8.2.2. В организации создается структурное подразделение и назначаются лица, ответственные за организацию планирования, совершенствования и развития обеспечения и управления ИБ в организации. Обязанности ответственных лиц определяются их должностными инструкциями.

8.2.3. При выборе средств обеспечения и контроля ИБ организация ориентируется на использование отечественных продуктов, в том числе на использование отечественного системного и прикладного ПО, вычислительной техники и сетевого оборудования.

8.3. **Аудит и контроль соблюдения требований ИБ**

8.3.1. Для оценки эффективности применяемых мер и средств обеспечения ИБ, а также пригодности и адекватности подхода к обеспечению ИБ, в организации периодически проводятся мероприятия по аудиту (проверке) ИБ.

8.3.2. При проведении аудитов ИБ используются процедуры документальной проверки, опрос и интервью с работниками организации, и технические процедуры тестирования (тестирование на проникновение и т.п.).

8.3.3. К проведению внутренних аудитов ИБ могут привлекаться специалисты, обладающие специальными навыками и знаниями, имеющими значение для проведения аудита.

8.4. **Управление доступом к информационным активам**

8.4.1. Управление доступом (в т.ч. удаленным) к информационным активам организации определяется принципами предоставления работникам и иным третьим лицам минимально необходимых для осуществления их деятельности привилегий.

8.4.2. Доступ к информационным активам организации предоставляется по согласованию с владельцем актива и подразделением информационной безопасности только на основании документально обоснованной производственной необходимости (подписанная служебная записка, электронное письмо, согласование в системе заявок и т.д.).

8.4.3. Доступ к информационным системам и ресурсам предоставляется только после успешного прохождения процедуры аутентификации.

8.5. **Защита от вредоносного ПО**

8.5.1. В организации реализуются меры защиты от вредоносного программного обеспечения для всех компонентов информационной инфраструктуры.

8.5.2. Внедряются меры обнаружения, предупреждения и восстановления последствий воздействия вредоносного ПО.

8.6. **Защита от утечек информации**

8.6.1. В организации осуществляются мероприятия для защиты информации от ее несанкционированного разглашения (утечки).

8.6.2. В рамках данных мероприятий осуществляется контроль следующей информации:

- информации, передаваемой во внутренней телекоммуникационной сети организации;
- информации, передаваемой в информационно-телекоммуникационную сеть «Интернет»;
- информации, передаваемой с использованием средств электронной почты;

- информации, передаваемой с использованием устройств мобильной связи, зарегистрированных в сети организации;
- информации, передаваемой на печать;
- информации, записываемой на съемные носители.

8.6.3. Распространение информации и передача информационных активов (за исключением общедоступной информации) запрещены, если только такое действие не осуществляется согласно случаям, предусмотренным законодательством Российской Федерации, нормативными документами регулирующих организаций, внутренними документами организации, включая Политику.

8.7. **Безопасность сетевой инфраструктуры**

8.7.1. В организации осуществляется управление безопасностью телекоммуникационных сетей организации и ее элементов, позволяющее обеспечить защиту информационных активов организации от угроз, включая постоянный мониторинг состояния безопасности сети.

8.7.2. Для удаленного доступа к телекоммуникационной сети организации применяется двухфакторная аутентификация.

8.7.3. При осуществлении удаленного доступа к ресурсам корпоративной сети организации применяется шифрование информации, передаваемой по общедоступным каналам связи.

8.8. **Криптографические меры защиты информации**

8.8.1. В целях защиты конфиденциальной информации в организации применяются средства криптографической защиты информации (далее – СКЗИ).

8.8.2. СКЗИ используются в соответствии с законодательством Российской Федерации и на основании технической и эксплуатационной документации, представляемой производителем СКЗИ.

8.8.3. Необходимость использования средств криптографической защиты информации определяется для каждого канала передачи информации, выходящего за пределы внутренней корпоративной сети организации.

8.9. **Управление уязвимостями**

8.9.1. В организации осуществляется процесс управления уязвимостями, включающий в себя постоянное выявление, анализ и устранение выявленных уязвимостей.

8.9.2. Проводятся регулярные работы по тестированию на проникновение в информационные ресурсы организации.

8.10. **Управление инцидентами ИБ**

8.10.1. В организации осуществляется процесс управления инцидентами ИБ, в рамках которого каждый инцидент ИБ должен фиксироваться и расследоваться.

8.10.2. Результаты служебного расследования докладываются руководству организации. По каждому случаю нарушения требований ИБ принимается решение о наложении на виновных лиц дисциплинарных взысканий.

8.11. **Управление изменениями**

8.11.1. В организации осуществляется процесс управления изменениями. Все изменения, вносимые в программное обеспечение ИС и оборудование, регистрируются и контролируются.

8.11.2. Определяются и сохраняются параметры безопасных конфигураций ИС и оборудования. Данные параметры в обязательном порядке применяются при настройке и восстановлении работоспособности оборудования и ИС.

8.12. **Резервное копирование и восстановление информации**

8.12.1. В организации выполняется регулярное резервное копирование информации, программного обеспечения и образов ИС.

8.12.2. Создаваемые резервные копии регулярно тестируются для обеспечения их целостности.

8.13. **Обеспечение соответствия требованиям в области ИБ**

8.13.1. Для выполнения всех обязательных требований по защите конфиденциальной информации, предписанных законодательными и другими регулирующими (нормативными) документами, в организации выполняется регулярный пересмотр документов по ИБ и содержащихся в них требований.

8.13.2. Руководители структурных подразделений организации в пределах своей области ответственности регулярно анализируют соответствие обработки информации и процедур требованиям внутренних документов организации по ИБ, в том числе требованиям Политики.

8.14. **Повышение осведомленности в области ИБ**

8.14.1. В организации осуществляется обучение и повышение осведомленности работников в области обеспечения ИБ.

8.14.2. Проводятся регулярные обучающие мероприятия для работников, а также иных третьих лиц, допущенных к информационным активам организации. По результатам проведенных мероприятий проводятся регулярные проверки полученных знаний.

8.15. **Обеспечение безопасности при взаимодействии с третьими лицами**

8.15.1. Меры безопасности при организации работ с третьими лицами и сторонними организациями предусматривают:

- определение и оценку потребностей организации в необходимости осуществления работ с привлечением сторонних организаций, а также проведение анализа и оценки рисков, являющихся следствием данного вида работ (в том числе определение критериев выбора и оценки сторонних организаций);
- постоянный контроль доступа третьих лиц и сторонних организаций к информационным активам организации и средствам ее обработки;
- осуществление допуска сторонних организаций и третьих лиц к информационным активам организации только после определения и реализации необходимых требований безопасности и ответственности за

их нарушение, а также включения таких требований в заключенные с указанными лицами и организациями договоры и соглашения;

- возможность на регулярной основе отслеживать и проводить аудит услуг, предоставляемых третьим лицом или сторонней организацией.

8.16. **Организация защиты персональных данных**

8.16.1. Персональные данные являются важным информационным активом организации, в связи с чем организация принимает меры по их защите в соответствии с требованиями законодательства Российской Федерации, нормативными документами регулирующих организаций.

8.16.2. Защита персональных данных обеспечивается путем организации корректной обработки, передачи и хранения персональных данных, а также комплексом организационных и технических мероприятий, направленных на обеспечение их безопасности.

8.17. **Организация физической защиты**

8.17.1. С целью предотвращения несанкционированного доступа в организации вводится пропускной режим и контроль физического доступа к информационным активам и компонентам ИТ-инфраструктуры, который осуществляется с использованием системы контроля и управления доступом (СКУД).

8.17.2. В зонах безопасности, а также во всех офисных, вспомогательных, подсобных, технических и т.п. помещениях реализуются меры по противопожарной защите, защите от аварий в системах электро-, тепло-, водо-, газоснабжения, канализации и стихийных бедствий.

8.18. **Применение технических средств защиты информации**

8.18.1. Технические средства защиты информации размещаются в информационной инфраструктуре организации и настраиваются в соответствии с требованиями эксплуатационной документации.

8.18.2. Для всех применяемых технических средств защиты информации обеспечивается возможность их поддержки (сопровождения) в течение всего срока использования.

8.18.3. Для нейтрализации актуальных угроз безопасности информации в соответствии с Моделью угроз организации, применяются технические средства защиты информации, сертифицированные ФСТЭК России по требованиям безопасности.

9. Ответственность

9.1. Директор организации при обеспечении ИБ в организации несет ответственность за:

- утверждение Политики и внутренних документов организации в части обеспечения ИБ;
- утверждение направлений развития ИБ в контексте снижения общих рисков Организации;

- выделение финансовых и материальных средств, а также кадровых ресурсов для организации обеспечения ИБ;
- утверждение организационной структуры подразделения ИБ;
- назначение ответственных лиц за обеспечение ИБ.

9.2. Заместитель директора по обеспечению информационной безопасности несет ответственность за:

- планирование, контроль, организацию и развитие мер обеспечения и управления ИБ в организации.

9.3. Подразделение информационной безопасности при обеспечении ИБ в организации несет ответственность за:

- разработку, документирование и внедрение мер обеспечения и управления ИБ;
- определение мер, необходимых для реализации планов и стратегий в части управления и защиты информации на каждом этапе ее обработки;
- анализ угроз и рисков ИБ, планирование и реализацию мероприятий по снижению угроз и управлению рисками;
- выполнение требований законодательства Российской Федерации, нормативных документов регулирующих организаций и иных применимых требований в области ИБ;
- контроль за применяемыми мерами ИБ и совершенствование применяемых мер;
- организацию обучения и повышения осведомленности работников в области ИБ.

9.4. Подразделение информационных технологий при обеспечении ИБ в организации несет ответственность за:

- поддержку и участие в процессах обеспечения ИБ, связанных с использованием информационных технологий;
- соблюдение установленных требований в части обеспечения ИБ при разработке, внедрении и эксплуатации информационных систем и информационных активов;
- участие в процессе анализа угроз и рисков ИБ, планирование и реализацию мероприятий по снижению угроз и управлению рисками совместно с подразделением информационной безопасности;
- планирование, реализацию мероприятий и бюджета, направленных на сопровождение закупок, эксплуатацию оборудования и информационных систем в целях информационной безопасности;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- предоставление информации о применяемых информационных технологиях и ИС подразделению информационной безопасности.

9.5. Руководители структурных подразделений организации при обеспечении ИБ в организации несут ответственность за:

- управление информационными активами, согласование прав доступа к информационным активам, принятие решений по рискам нарушения ИБ, связанным с информационными активами;
- доведение требований по обеспечению ИБ до работников подчиненных структурных подразделений;
- своевременное информирование подразделения информационной безопасности о выявленных рисках и инцидентах информационной безопасности;
- исполнение требований подразделения информационной безопасности по минимизации рисков ИБ, устранению условий и последствий инцидентов.

9.6. Работники организации при обеспечении ИБ в организации несут ответственность за:

- исполнение требований внутренних документов организации в части обеспечения ИБ.

10. Заключительные положения

10.1. Настоящая Политика подлежит регулярному пересмотру не реже 1 раза в 3 года, а также в следующих случаях:

- изменения требований законодательства Российской Федерации, нормативных документов регулирующих органов;
- существенных изменений в информационной инфраструктуре или организационной структуре организации;
- выявления инцидентов ИБ, свидетельствующих о неполноте или несовершенстве настоящей Политики.

10.2. Предпосылками для пересмотра и совершенствования настоящей Политики могут также являться результаты мониторинга состояния ИБ, результаты анализа актуальных внутренних и внешних угроз, а также результаты анализа нарушений, выявленных в ходе внутреннего и внешнего контроля (несоответствие реальных технологий и состояния информационной безопасности требованиям нормативных и регламентирующих документов).

10.3. Политика должна быть доведена до всех работников и принята ими к обязательному исполнению. Политика также должна быть доведена до контрагентов и иных третьих лиц, допущенных к информационным активам организации, и принята ими к обязательному исполнению в части, их касающейся.

10.4. Все работники организации, а также иные третьи лица при обращении с информационными активами организации должны руководствоваться утвержденными требованиями организационно-распорядительных, эксплуатационных, методических и иных документов, связанных с обеспечением ИБ, в том числе требованиями Политики.

10.5. За нарушение требований в области ИБ работники организации несут персональную ответственность в соответствии с законодательством Российской Федерации.

10.6. Ответственность за осуществление общего контроля выполнения Политики, предоставление рекомендаций по их выполнению, поддержание Политики в актуальном состоянии с учетом требований международных и национальных стандартов, а также законодательства Российской Федерации, нормативных документов регулирующих организаций несет заместитель директора организации по обеспечению информационной безопасности.

10.7. Настоящая Политика, а также все изменения к ней утверждаются приказом директора организации и вступают в силу после его опубликования.

11. Нормативные документы

11.1. При разработке настоящей Политики использовались следующие нормативные документы:

- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ;
- Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ;
- Указ Президента РФ от 5.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации";
- Указ Президента РФ от 1.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации";
- Постановление Правительства РФ от 15.07.2022 № 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)".