1. **Основные положения.**
   1. Настоящая политика разработана в соответствии с законодательством РФ, в частности с законом «О государственной тайне» от 21 июля 1993 года №5485-1.
   2. Настоящая политика – документ, доступный любому сотруднику института, содержащий информацию о защите данных научных исследований, а также о степени доступности информации сотрудникам НИИ.
   3. Защита информационной безопасности научно-исследовательского института лежит в юрисдикции ФСБ.
   4. Все требования обеспечения информационной безопасности должны соблюдаться сотрудниками непрекословно.
   5. Все сотрудники, имеющие доступ к уровню А-2 и выше обязаны ознакомиться с расширенной версией политики безопасности.
   6. Все изменения в данной политике безопасности должны быть согласованны с администрацией президента.
2. **Список терминов и определений.**

В данном разделе указаны все термины, сокращения и их определения, необходимые для понимания нижеизложенной информации.

2.1. НИИ - научно-исследовательский институт государственное учреждение, специально созданное для организации научных исследований и проведения опытно-конструкторских разработок.

2.2. Гос. – «государство» и все производные от него слова.

2.3 ИБ – информационная безопасность.

1. **Описание объекта защиты.**

Основными объектами защиты системы информационной безопасности являются:

* Информационные ресурсы, содержащие информацию о работе НИИ
* Информационные ресурсы, содержащие гос. тайну
* Информационные ресурсы, содержащие информацию о сотрудниках НИИ, их разработках и деятельности вне лаборатории
* Все виды информационных носителей, в любой мере связанные с работай НИИ
* Сотрудники, работающие в текущий момент или работавшие в НИИ в любой период на протяжении последних тридцати лет

1. **Цели и задачи по обеспечению информационной безопасности.**

Целью деятельности по обеспечению информационной безопасности НИИ является устранение всех возможных внешних и внутренних угроз.

Основные задачи деятельности по обеспечению ИБ НИИ:

* Защита информации от утечек
* Выявление потенциальных угроз ИБ и уязвимостей объектов защиты
* Предотвращение инцидентов ИБ
* Исключение выявленных угроз

1. **Угрозы информационной безопасности.**

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

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 НИИ и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и 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 (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре НИИ могут быть как внешними, так и внутренними.

1. **Модель нарушителя информационной безопасности.**

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

* 1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей НИИ рассматриваются:

* Сотрудники НИИ, не допущенные к ресурсам информационных систем, но имеющие доступ в здания и помещения;
* Персонал, обслуживающий технические средства корпоративной информационной системы НИИ;
* Сотрудники самостоятельных структурных подразделений НИИ, задействованные в разработке и сопровождении программного обеспечения;
* Сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность НИИ;
* Руководители различных уровней
  1. Внешние нарушители.

В качестве потенциальных внешних нарушителей рассматриваются:

* бывшие сотрудники НИИ;
* представители организаций, взаимодействующих по вопросам технического обеспечения НИИ и поставки необходимых объектов;
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
* лица, случайно или умышленно проникшие в корпоративную информационную систему из внешних телекоммуникационных сетей (хакеры).
  1. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:
* нарушитель скрывает свои несанкционированные действия от других сотрудников НИИ;
* несанкционированные действия нарушителя могут быть следствием ошибок сотрудников, 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 НИИ обязательны к соблюдению всеми сотрудниками.

7.2. Работа по обеспечению информационной безопасности сотрудниками иных сфер и направлений приветствуется и поощряется в установленном порядке.

7.3. Неисполнение или некачественное исполнение сотрудниками обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным уголовных мер воздействия, степень которых определяется требованиями действующего законодательства.

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

7.4.1. Определение и распределение ролей персонала, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

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

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

**8. Организационная основа деятельности по обеспечению информационной безопасности**

8.1. В целях выполнения задач по обеспечению информационной безопасности в НИИ должны быть назначены:

* Куратор;
* Ответственное подразделение;

При необходимости могут быть назначены и другие группы по информационной безопасности.

8.2. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые сотрудником Ответственного подразделения, и может, при наличии обоснованной необходимости по согласованию с администрацией президента, привлекать для работы в них сотрудников других самостоятельных структурных подразделений НИИ на основе совмещения работы в группе со своими основными должностными обязанностями.

8.4. Финансирование работ по реализации положений настоящей Политики осуществляется в рамках гос. финансирования.

8.5. Полные полномочия и функции куратора и ответственного подразделения описаны в расширенной версии политики безопасности.

**9. Ответственность за соблюдение положений Политики.**

Общее руководство обеспечением информационной безопасности НИИ осуществляет Куратор. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности НИИ лежит на руководстве Ответственного подразделения.

Ответственность работников НИИ за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками, а также положениями внутренних нормативных документов.

**10. Контроль за соблюдением положений Политики.**

Общий контроль состояния информационной безопасности НИИ осуществляется Куратором. Текущий контроль соблюдения настоящей Политики осуществляет Ответственное подразделение. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий. Департамент внутреннего контроля осуществляет контроль соблюдения настоящей Политики на основе проведения внутреннего аудита информационной безопасности.

**11. Заключительные положения.**

11.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами, которые дополняют и уточняют ее.

11.2. В случае изменения действующего законодательства и иных нормативных актов, настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

11.3. Ответственным за внесение изменений в настоящую Политику является руководитель Ответственного подразделения.