**Общество с ограниченной ответственностью**

**«ИнноСофт»**

УТВЕРЖДАЮ

Генеральный директор

ООО «ИнноСофт»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Тазеев Р.Р.

\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_202\_\_ г.

**Политика информационной безопасности ООО "ИнноСофт".**

**Дата введения \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Издание №\_\_\_\_\_**

Настоящий документ не может быть полностью или частично воспроизведен, тиражирован и распространен без разрешения ООО «ИнноСофт»

2024

ИНФОРМАЦИОННЫЕ ДАННЫЕ

ВВЕДЕНО В ДЕЙСТВИЕ ПРИКАЗОМ №\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_20\_\_г.

РАЗРАБОТАНО: Отдел защиты информации

ИСПОЛНИТЕЛИ:

Начальник отдела защиты информации Тазеев Р.Р. \_\_\_\_\_\_\_\_

СОГЛАСОВАНО:

Директор департамента ИТ Тазеев Р.Р. \_\_\_\_\_\_\_\_

Начальник юридической службы Тазеев Р.Р. \_\_\_\_\_\_\_\_

Директор финансового департамента Тазеев Р.Р. \_\_\_\_\_\_\_\_

**СОДЕРЖАНИЕ**

[1. ОБЩИЕ ПОЛОЖЕНИЯ 4](#_Toc477876072)

[2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 6](#_Toc477876073)

[3. СПИСОК ИСПОЛЬЗОВАНЫХ СОКРАЩЕНИЙ 10](#_Toc477876074)

[4. ЦЕЛИ ПОЛИТИКИ 11](#_Toc477876075)

[5. ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 12](#_Toc477876076)

[6. ОБЛАСТЬ ПРИМЕНЕНИЯ 16](#_Toc477876077)

[7. ОСНОВНЫЕ ЗАДАЧИ 17](#_Toc477876078)

[8. УГРОЗЫ И ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 20](#_Toc477876079)

[9. УПРАВЛЕНИЕ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 22](#_Toc477876080)

[10. ОТВЕТСТВЕННОСТЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 30](#_Toc477876083)

[11. НОРМАТИВНЫЕ ССЫЛКИ 31](#_Toc477876084)

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Политика информационной безопасности (далее – Политика) ООО «ИнноСофт» (далее – Общество) представляет собой совокупность управленческих решений, лежащих в основе организационно-распорядительных документов, регламентирующих правила и нормы информационной безопасности, применяемые в процессе разработки программного обеспечения.

1.2. Настоящая Политика является официально принятой руководством Общества системой взглядов на проблему обеспечения информационной безопасности, определяет основные направления деятельности руководящего состава Общества по устранению потенциальных угроз информационной безопасности в процессе разработки и эксплуатации программных продуктов, содержит цели, задачи и принципы достижения требуемого уровня безопасности информации, определяет виды угроз безопасности информации и информационные ресурсы, подлежащие защите.

1.3. Политика является внутренним документом верхнего уровня в системе организационно-нормативного обеспечения защиты информации в информационных системах Общества. Организационно-нормативные документы нижнего уровня создаются в развитие Политики, определяя и уточняя процедуры и порядки, направленные на реализацию положений Политики.

1.4. Основу политики информационной безопасности составляет:

* соответствие процессов сбора, накопления, обработки, предоставления и распространения информации требованиям ратифицированного в Российской Федерации международного законодательства, законодательства Российской Федерации, требованиям и нормативным документам регуляторов, а также собственным приоритетам в вопросах защиты интеллектуальной собственности;
* централизованная разработка документов Общества, регламентирующих вопросы информационной безопасности, обязательность выполнения их требований;
* единство технической политики Общества в области реализации технических, программных и программно-технических мер по защите информационных ресурсов и технологий, используемых в разработке программного обеспечения;
* персональная ответственность сотрудников за нарушения в сфере информационной безопасности;
* обеспечение постоянного контроля состояния информационной безопасности в Обществе.

1.5. Информация, обрабатываемая и используемая в Обществе, является одним из ценных активов и, следовательно, нуждается в соответствующей защите. Несанкционированное изменение, недоступность информации для принятия решений и осуществления бизнес-процессов, а также несанкционированный доступ к информации, конфиденциальность которой определена руководством Общества и (или) требованиями законодателя и регуляторов, могут привести к материальному ущербу для Общества и его сотрудников, а также к ухудшению репутации Общества.

1.6. За разработку, принятие, внедрение и реализацию Политики отвечает начальник отдела информационной безопасности.

**2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

2.1. **Администратор безопасности** – функциональная роль в информационной системе, отвечающая за информационную безопасность в этой системе и имеющая право назначать иные роли и распределять права доступа.

2.2. **Безопасность информации** – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз, в том числе в процессе разработки программного обеспечения.

2.3. **Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной и контрразведывательной деятельности, распространение которых может нанести ущерб безопасности государства.

2.4. **Доступ к информации** – возможность получения информации и её использования в рамках разработки и эксплуатации программного обеспечения.

2.5. **Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию в процессе работы над программными продуктами.

2.6. **Защищаемая информация** – информация, являющаяся предметом собственности Общества и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

2.7. **Информационная безопасность** – в рамках данного документа под информационной безопасностью понимается непрерывный во времени процесс обеспечения конфиденциальности, целостности и доступности защищаемой информации, включая информацию, связанную с разработкой ПО.

2.8. **Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств, используемых в процессе разработки программного обеспечения.

2.9. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, применяемых в Общества.

2.10. **Информационный процесс** – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации, включая информацию, связанную с программными продуктами.

2.11. **Информация** – сведения (сообщения, данные) независимо от формы их представления, используемые в процессе разработки и эксплуатации ПО.

2.12. **Инцидент информационной безопасности (Инцидент ИБ)** – единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое может скомпрометировать бизнес-процессы Общества или угрожает её информационной безопасности, особенно в рамках разработки программного обеспечения.

2.13. **Коммерческая тайна** – информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам и которая является предметом защиты в соответствии с законодательством Российской Федерации.

2.14. **Контролируемая зона** – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

2.15. **Конфиденциальная информация** – информация с ограниченным доступом, накопленная в процессе разработки программного обеспечения и являющаяся собственностью Общества.

2.16. **Конфиденциальность персональных данных** – обязательное для соблюдения требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

2.17. **Модель угроз (безопасности информации)** – физическое, математическое или описательное представление свойств или характеристик угроз безопасности информации, актуальных для разработки ПО.

2.18. **Мультисервисная сеть предприятия** – универсальная многоцелевая среда, предназначенная для передачи речи, изображения и данных с использованием технологии коммутации пакетов, используемая в рамках деятельности Общества.

2.19. **Несанкционированный доступ к информации** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами информационных систем Общества.

2.20. **Носитель защищаемой информации** – физическое лицо или материальный объект, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.21. **Обработка персональных данных** – любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без таковых с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, использование, передачу и уничтожение персональных данных.

2.22. **Оператор** – юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и осуществляющее обработку персональных данных, включая данные пользователей программного обеспечения.

2.23. **Персональные данные** – любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу, включая информацию о пользователях программного обеспечения.

2.24. **Подсистема информационной безопасности** – структурная часть общей системы информационной безопасности Общества, служащая для реализации технических защитных мер в отношении разработанных программных продуктов и связанных информационных систем.

2.25. **Режим коммерческой тайны** – режим конфиденциальности информации, позволяющий её обладателю защитить коммерческие интересы в условиях конкуренции.

2.26. **Сертификация на соответствие требованиям по безопасности информации** – форма подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным стандартами или условиями договоров.

2.27. **Средство защиты информации** – техническое и/или программное средство, предназначенное или используемое для защиты информации, включая программные продукты.

2.28. **Система обеспечения информационной безопасности** – функционирующая как единое целое совокупность средств и мероприятий, направленных на защиту информации в процессе разработки и эксплуатации программного обеспечения.

**3. СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ**

3.1. **АРМ** – автоматизированное рабочее место.  
3.2. **ИС** – информационная система.  
3.3. **ИСПДн** – информационная система, содержащая персональные данные.  
3.4. **КЗ** – контролируемая зона.  
3.5. **КТ** – коммерческая тайна; информация, составляющая коммерческую тайну.  
3.6. **МСС** – мультисервисная сеть.  
3.7. **ОЗИ** – отдел защиты информации.  
3.8. **ОС** – операционная система.  
3.9. **НСД** – несанкционированный доступ к информации.  
3.10. **ПДн** – персональные данные.  
3.11. **ПИБ** – подсистема информационной безопасности.  
3.12. **ПО** – программное обеспечение.  
3.13. **Пользователи ИС** – сотрудники Общества, использующие информационные системы в процессе выполнения своих должностных обязанностей.  
3.14. **СВТ** – средство вычислительной техники.  
3.15. **СОИБ** – система обеспечения информационной безопасности.  
3.16. **СКЗИ** – средство криптографической защиты информации.  
3.17. **СТР-К** – Специальные требования и рекомендации по технической защите конфиденциальной информации, одобренные решением коллегии Гостехкомиссии России от 02.03.2001 г.  
3.18. **ТЗ** – техническое задание.  
3.19. **ФСБ России** – Федеральная служба безопасности Российской Федерации.  
3.20. **ФСТЭК России** – Федеральная служба по техническому и экспортному контролю Российской Федерации.

**4. ЦЕЛИ ПОЛИТИКИ**

4.1. Политика информационной безопасности (далее – Политика) представляет собой систематизированное изложение целей и задач защиты, основных принципов построения системы информационной безопасности, требований к организационным и техническим мерам защиты информации в информационных системах ООО «ИнноСофт».  
4.2. Целями разработки и применения Политики являются:

1. защита интересов ООО «ИнноСофт» от актуальных угроз информационной безопасности путем их исключения или минимизации;
2. определение стратегии построения, реализации и дальнейшего развития системы информационной безопасности информационных систем Общества;
3. формирование требований по защите информационных систем Общества, единых для всех подразделений;
4. выполнение требований действующего законодательства, подзаконных актов и требований профильных регуляторов в сфере информационной безопасности;
5. применение лучших мировых практик в области защиты информации и обеспечения непрерывности критически важных технологических процессов.
6. **ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

При достижении поставленных целей ООО «ИнноСофт» намерено руководствоваться следующими принципами:

5.1. **Законность.** Осуществление защитных мероприятий и разработка системы безопасности информации в Обществе будет проводиться в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также другими нормативными актами по безопасности, утверждёнными органами государственной власти.

5.2. **Системность.** Системный подход к защите информации предполагает учёт всех взаимосвязанных и изменяющихся элементов и факторов, значимых для обеспечения информационной безопасности в Обществе. При создании системы защиты должны учитываться все уязвимые места, а также возможные направления атак на систему.

5.3. **Комплексность.** Использование разнородных средств защиты при построении целостной системы защиты, которая перекрывает все значимые векторы угроз информационной безопасности и не содержит слабых мест на стыках компонентов. Защита должна строиться эшелонировано, включая физические, организационные, технологические и правовые меры.

5.4. **Непрерывность защиты.** Защита информации – это непрерывный процесс, включающий меры на всех этапах жизненного цикла информационных систем Общества, начиная с проектирования и заканчивая эксплуатацией.

5.5. **Своевременность.** Упреждающий характер мер безопасности, реализация которых должна начинаться на ранних стадиях разработки информационных систем и их систем информационной безопасности.

5.6. **Преемственность и совершенствование.** Постоянное совершенствование мер и средств защиты информации на основе анализа функционирования систем и изменений в методах перехвата информации, а также учёт лучших практик.

5.7. **Разумная достаточность.** Соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их утраты или искажения. Меры безопасности не должны ухудшать эргономические показатели работы информационных систем.

5.8. **Персональная ответственность.** Ответственность за обеспечение безопасности информации возлагается на каждого сотрудника в пределах его полномочий. Распределение прав и обязанностей должно минимизировать круг виновников в случае нарушения.

5.9. **Минимизация полномочий.** Предоставление пользователям минимальных прав доступа, необходимых для выполнения их служебных обязанностей.

5.10. **Открытость алгоритмов и механизмов защиты.** Защита не должна основываться исключительно на секретности алгоритмов; знание их не должно давать возможности преодоления системы защиты.

5.11. **Специализация и профессионализм.** Привлечение к разработке и реализации мер защиты информации сотрудников с соответствующим образованием и опытом.

5.12. **Обязательность контроля.** Обязательность выявления и пресечения нарушений правил обеспечения безопасности информации на основе систем и средств контроля.

5.13. **Вовлеченность руководства.** Активное участие руководства Общества в обеспечении информационной безопасности, включая соблюдение тех же правил, что и все сотрудники.

**6. ОБЛАСТЬ ПРИМЕНЕНИЯ**

6.1. Положения настоящей Политики распространяются на всех работников ООО «ИнноСофт», имеющих доступ к информационным активам и ИТ-инфраструктуре Общества, а также учитываются в отношениях с контрагентами, включая потребителей продукции, поставщиков, партнеров, консультантов, стажеров и практикантов.

6.2. В общем случае предметом настоящей Политики являются информация или носитель защищаемой информации, либо информационный процесс, который необходимо защищать в соответствии с целями Политики. Основным объектом защиты является информация; необходимость защиты носителей информации и информационных процессов вытекает из необходимости защиты информации.

6.3. Информация, обрабатываемая в Обществе, делится на следующие категории:

* Персональные данные;
* Коммерческая тайна;
* Иная информация, не отнесенная к предыдущим категориям.

6.4. В соответствии с целями Политики к объектам защиты следует относить:

* Средства и системы информатизации, используемые для обработки защищаемой информации;
* Технические средства и системы, которые не обрабатывают непосредственно защищаемую информацию, но размещены в помещениях, где она обрабатывается;
* Любые носители информации, в том числе не относящиеся к системам автоматизированной обработки информации;
* Защищаемые помещения.

**7. ОСНОВНЫЕ ЗАДАЧИ**

7.1. Основными задачами Политики являются:

* Определение единых для всех информационных систем (ИС) Общества подходов к обеспечению информационной безопасности, обеспечивающих необходимый уровень защиты информационных ресурсов;
* Обеспечение выполнения в Обществе требований законодательства Российской Федерации по защите информации;
* Защита конфиденциальной информации Общества;
* Создание основы для проведения единой технической политики в области применения информационных технологий и создания единой системы обеспечения информационной безопасности (СОИБ) в Обществе.

7.2. Для достижения целей Политики и обеспечения безопасности информации СОИБ Общества должно эффективно решать следующие задачи:

* Своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений и нарушению нормального функционирования ИС и подразделений Общества;
* Управление инцидентами информационной безопасности;
* Повышение уровня осведомленности сотрудников Общества в области информационной безопасности;
* Создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
* Создание условий для минимизации и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
* Защита от вмешательства в процесс функционирования информационных систем Общества посторонних лиц (доступ к защищаемым ИС Общества должен иметь только зарегистрированные в установленном порядке пользователи);
* Разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Общества (доступ только к тем ресурсам и выполнение только тех операций с ними, которые необходимы для выполнения служебных обязанностей);
* Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* Защита от несанкционированной модификации программных средств, используемых в информационных системах Общества, а также защита от внедрения несанкционированных программ, включая компьютерные вирусы;
* Защита информации ограниченного доступа от утечки по любым каналам при её обработке, хранении и передаче по каналам связи;
* Обеспечение жизненного цикла средств криптографической защиты информации (СКЗИ) в соответствии с требованиями законодательства и регуляторов;
* Обеспечение восстановления работы защищаемых ИС Общества в случае возникновения инцидента информационной безопасности;
* СОИБ Общества должна полностью соответствовать требованиям действующего законодательства в вопросах защиты коммерческой тайны, персональных данных и требованиям профильных нормативно-правовых и методических документов регуляторов;
* СОИБ Общества должна использовать передовые мировые практики в вопросах разработки, внедрения и управления системами информационной безопасности, не нарушая требования предыдущего подпункта.

7.3. Действенность системы обеспечения информационной безопасности Общества достигается установлением порядка, правил и зон ответственности в сфере защиты информации, которые должны определять цели и содержание деятельности Общества по обеспечению управления информационной безопасностью.

7.4. Для достижения поставленных целей и эффективного выполнения задач по обеспечению информационной безопасности в Обществе определяется совокупность индивидуальных правил, устанавливающих допустимое взаимодействие между работником и объектами информатизации.

7.5. Правила должны быть персонифицированы для каждого работника в виде обязанностей с установлением ответственности за их исполнение. Ответственность за надлежащее исполнение обязанностей должна быть закреплена в должностной инструкции каждого работника.

7.6. Исполнение обязанностей по информационной безопасности работников Общества должно быть обеспечено необходимыми ресурсами.

7.7. Не должно допускаться совмещение обязанностей работника, включающих функции сопровождения, исполнения, администрирования, с обязанностями, включающими функции контроля.

**8. УГРОЗЫ И ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

8.1. Угроза информационной безопасности — это совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

8.2. Угрозы информационной безопасности Общества подлежат классификации по следующим признакам:

* **По аспекту информационной безопасности, на который направлены угрозы:**
  + Угрозы конфиденциальности (неправомерный доступ к информации).
  + Угрозы целостности (неправомочное изменение данных).
  + Угрозы доступности (действия, делающие невозможным или затрудняющим доступ к ресурсам информационной системы).
* **По степени преднамеренности действий:**
  + Случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия).
  + Преднамеренные (умышленные действия, например, шпионаж и диверсии).
* **По расположению источника угроз:**
  + Внутренние (источники угроз располагаются внутри системы).
  + Внешние (источники угроз находятся вне системы).
* **По размерам наносимого ущерба:**
  + Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба).
  + Локальные (причинение вреда отдельным частям объекта безопасности).
  + Частные (причинение вреда отдельным свойствам элементов объекта безопасности).
* **По степени воздействия на информационную систему:**
  + Пассивные (структура и содержание системы не изменяются).
  + Активные (структура и содержание системы подвергается изменениям).

8.3. Объектами угроз информационной безопасности Общества являются все виды информации, указанные в пункте 6.3 Политики.

8.4. При определении угроз необходимо руководствоваться:

* Для коммерческой тайны — требованиями, указанными в пунктах 11.20 и 11.29 Политики;
* Для персональных данных — методикой, указанной в пункте 11.19 Политики;
* Для иной защищаемой информации, защита которой не является обязательной с точки зрения законодателя и регуляторов — перечень актуальных угроз определяется экспертным методом с применением наиболее подходящих из существующих руководящих документов (например, те, которые определены для коммерческой тайны).

8.5. Перечень нормативных ссылок, указанный в пункте 8.4, не является исчерпывающим. При проведении работ по моделированию угроз безопасности информации необходимо применять наиболее актуальные на момент выполнения работ руководящие документы.

**9. УПРАВЛЕНИЕ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**9.1. Направления обеспечения информационной безопасности в информационных системах**

**9.1.1. Общие положения**  
Информационная безопасность информационных систем обеспечивается на всех стадиях их жизненного цикла с учетом степени участия в этом процессе субъектов отношений в информационной сфере (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и иных организаций).

**9.1.2. Процесс создания информационных систем включает:**

* Обоснованную формулировку требований к обеспечению информационной безопасности, соответствующую действующей нормативной базе и значимости защищаемой информации.
* Выбор оптимальных проектных решений и адекватной модели жизненного цикла.
* Разработку необходимой эксплуатационной документации и организационно-распорядительных документов, регламентирующих порядок работы с защищаемой информацией.
* Приемку в эксплуатацию (при необходимости, с проведением установленных проверок).
* Оценку соответствия выбранных мер защиты информации установленным требованиям ИБ.
* Предотвращение внесения недокументированных возможностей в программное обеспечение и оборудование.

**9.1.3. В процессе эксплуатации информационных систем обеспечивается защита от:**

* Несанкционированного доступа к информации, её модификации или уничтожения.
* Неумышленной модификации или уничтожения информации.
* Недоставки или ошибочной доставки информации.
* Отказа в обслуживании или ухудшения обслуживания.
* Отказа от авторства.  
  Недопустимо внесение изменений в автоматизированные системы и вычислительные сети, которые могут привести к нарушению их функциональности или появлению недокументированных возможностей.

**9.1.4. На стадии вывода из эксплуатации информационных систем обеспечивается:**

* Удаление информации из запоминающих устройств, несанкционированное использование которой может нанести ущерб коммерческой деятельности Общества.

**9.1.5. Требования по информационной безопасности включаются в:**

* Договоры и контракты на проведение работ или оказание услуг, заключаемые на всех стадиях жизненного цикла информационных систем, а также в соответствующую проектную документацию.

**9.1.6. Разработка и создание информационных систем, обрабатывающих информацию, доступ к которой ограничен федеральными законами, осуществляется в соответствии с требованиями нормативных актов и методических документов (ФСБ России и ФСТЭК России).**

**9.2. Меры по обеспечению информационной безопасности в информационных системах**

**9.2.1. В общем случае реализация требований Политики состоит из следующих шагов:**

* Разработка внутренних организационно-распорядительных документов, регламентирующих обработку защищаемой информации.
* Реализация организационных мер защиты информации.
* Оценка состояния защищенности ИС, разработка ТЗ на ПИБ.
* Реализация технических мер защиты информации с последующей оценкой их эффективности.
* Систематическая работа по уточнению набора мер и оценки эффективности как отдельных ПИБ, так и всей системы ИБ в целом.

**9.2.2. Реализация организационных мер защиты информации:**

* Основные задачи:
  + Формирование и совершенствование элементов системы обеспечения информационной безопасности.
  + Обеспечение соответствия организации защиты информации установленным требованиям.
  + Реализация единой технической политики безопасности информации.
  + Мониторинг внутренних и внешних условий функционирования объектов защиты, анализ эффективности управления защитой информации и подготовка решений по корректировке.
* Основные участники:
  + Генеральный директор Общества.
  + Начальник отдела защиты информации.
  + Начальник юридического отдела.
  + Начальник отдела информационных технологий.

**9.2.3. Разработка внутренних организационно-распорядительных документов:**

* Для обеспечения деятельности по защите информации в Обществе должны быть разработаны следующие документы (список не является исчерпывающим):
  + Положение об ответственном за защиту информации в Обществе.
  + Стандарты предприятия по информационной безопасности.
  + Документы, устанавливающие режим КТ.
  + Документы, регламентирующие порядок обработки ПДн.
  + Модели угроз.
  + Частные ТЗ на ПИБ для каждой ИС.

**9.2.4. Технические меры по защите информации:**

* Технические меры, предпринимаемые для защиты информационных систем, осуществляются с учетом основных принципов:
  + Обладания полномочиями, необходимыми для решения задач пользователем.
  + Разделения информационных ресурсов по степени доступности.
  + Разделения информационной инфраструктуры на сегменты с построением ПИБ для каждого сегмента.

**9.2.5. Планирование мероприятий информационной безопасности:**

* Основные документы планирования:
  + Комплексный план мероприятий ИБ на календарный год (далее – Комплексный план).
* Процесс разработки:
  + Комплексный план разрабатывается ОЗИ с 1 по 30 июля каждого года.
  + Проходит согласование с 1 по 30 августа и должен быть утвержден генеральным директором до 30 августа.
* Состав разделов Комплексного плана:
  + Организаторская работа руководства.
  + Подготовка персонала по вопросам защиты информации.
  + Контроль защиты информации.
  + Допуск и доступ персонала к различным категориям информации.
  + Поддержание режима КТ.
  + Защита информации при рекламной и публикаторской деятельности.
  + Защита информации при использовании технических средств.
  + Защита информации при международном сотрудничестве.
  + Защита информации при выполнении совместных работ.
  + Защита информации в чрезвычайных ситуациях.
  + Аналитическая работа на предприятии.

### **10. ОТВЕТСТВЕННОСТЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**10.1.** На начальника юридического отдела возлагается ответственность за контроль организации обработки защищаемой информации в соответствии с требованиями настоящей Политики.

**10.2.** На начальника ОЗИ возлагается ответственность за:

* организацию обработки защищаемой информации (как с применением средств автоматизации, так и без них) в соответствии с требованиями настоящей Политики, в том числе разработку документов на основе Политики, планирование мероприятий, согласование документов, влияющих на информационную безопасность;
* контроль исполнения требований Политики в структурных подразделениях Общества.

**10.3.** На руководителей структурных подразделений Общества возлагаются обязанности по обеспечению соблюдения установленного порядка обращения с защищаемой информацией в подчиненных им структурных подразделениях.

**10.4.** На начальника отдела информационных технологий возлагается ответственность за контроль соблюдения требований Политики и иных организационно-распорядительных документов Общества сотрудниками Общества при автоматизированной обработке защищаемой информации на рабочих местах.

**10.5.** Каждый работник Общества, имеющий доступ к защищаемой информации, несет ответственность за её искажение, разглашение и утрату, а также за нарушение установленного порядка обеспечения информационной безопасности.

**10.6.** Работники Общества, разгласившие защищаемую в Обществе конфиденциальную информацию или нарушившие установленный порядок обращения с защищаемой информацией, а также работники, по вине которых произошла утрата конфиденциальных документов, нарушение работы информационных систем, ухудшающее доступность, целостность, конфиденциальность защищаемой информации, несут ответственность, предусмотренную законодательством Российской Федерации, внутренними документами Общества.

**11. НОРМАТИВНЫЕ ССЫЛКИ**

**11.1 Международные документы**

* Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 (ратифицирована ФЗ от 19.12.2005 №160-ФЗ).

**11.2 Конституционные и стратегические документы**

* Конституция РФ;
* Доктрина информационной безопасности РФ (утверждена Президентом РФ 09.09.2000 № Пр.-1895).

**11.3 Федеральные законы**

* Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

**11.4 Постановления Правительства РФ**

* Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* (и т.д.).

**11.5 ГОСТы**

* ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения»;
* ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
* (и т.д.).

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Основание для изменений  (дата, № документа) | Номера листов | | | Дата внесе-ния измене-ний | Дата введе-ния измене-ний в дейст-вие | Всего листов в доку-менте | Фамилия лица, ответственного за внесение изменений |
| Изменен-ных | Новых | Анну-ли-рован-ных |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |