Введение

1.1. Цели и задачи информационной политики

1.2. Область применения

1.3. Определения и термины

Политики , положения и стратегии

11.1. Политика информационной безопасности организации

11.2. Политика защиты персональных данных

11.3. Политика реагирования на компьютерные инциденты

11.4. Стратегия развития информационной безопасности

11.5. Стратегия защиты критической информационной инфраструктуры

Положения об отделе ИБ

12.1. Положение об отделе информационной безопасности

12.2. Положение о службе реагирования на инциденты информационной безопасности

Обязанности и ответственность

2.1. Ответственность руководства

2.2. Ответственность сотрудников

2.3. Ответственные лица и органы

Права доступа и защита данных

3.1. Правила доступа

3.2. Защита конфиденциальности данных

3.3. Хранение и передача данных

Процедуры обработки и защиты данных

4.1. Сбор и обработка данных

4.2. Хранение данных

4.3. Уничтожение данных

Мониторинг и контроль

5.1. Контроль исполнения

5.1.1. Механизмы контроля

5.1.2. Регулярные отчеты

5.1.3. Внедрение систем контроля

5.1.4. Обратная связь и корректирующие действия

5.2. Аудит и проверка

5.2.1. Регулярные проверки и аудит

5.2.2. Оценка результатов

5.3. Выявление и устранение нарушений

5.3.1. Анализ нарушений

5.3.2. Корректирующие действия

5.3.3. Мониторинг исправлений

5.4. Отчетность и улучшение

5.4.1. Отчеты о результатах аудита

5.4.2. Периодический пересмотр

Обучение и повышение квалификации

6.1. Разработка и внедрение программ обучения

6.1.1. Основные курсы

6.1.2. Специальные тренинги

6.1.3. Методические материалы

6.1.4. Обучение по новым технологиям

6.2. Форматы обучения

6.2.1. Очное обучение

6.2.2. Дистанционное обучение

6.2.3. Практические занятия

6.3. Оценка и сертификация

6.3.1. Оценка знаний

6.3.2. Сертификация

6.4. Повышение квалификации

6.4.1. Мероприятия по повышению квалификации

6.4.2. Индивидуальное развитие

6.4.3. Оценка и улучшение

Права и обязанности

7.1. Доступ к данным

7.1.1. Определение прав

7.1.2. Права на доступ

7.2. Использование информации

7.2.1. Цели использования

7.2.2. Ограничения

7.3. Запросы и отчеты

7.3.1. Запрос информации

7.3.2. Отчеты

7.4. Обязанности сотрудников

7.4.1. Соблюдение Политики

7.4.2. Доклады о проблемах и предложениях

Использование ресурсов

8.1. Правильное использование

8.2. Отчетность

Мероприятия при обнаружении нарушений в сфере сохранности информации

9.1. Определение видов нарушений

9.1.1. Нарушение конфиденциальности

9.1.2. Нарушение процедур обработки данных

9.1.3. Необоснованный доступ

9.1.4. Неисполнение требований безопасности

9.1.5. Нарушение общих правил безопасности

9.2. Меры ответственности

9.2.1. Дисциплинарные последствия

9.2.2. Юридические последствия

9.2.3. Проведение расследования

9.2.4. Документирование

9.2.5. Процедура обжалования

9.3. Корректирующие действия

9.3.1. Устранение последствий

9.3.2. Обучение и повышение квалификации

Обновление и пересмотр политики

10.1. Основания для обновления

10.1.1. Изменения в законодательстве

10.1.2. Изменения в организационной структуре

10.1.3. Технологические новшества

10.1.4. Анализ инцидентов и нарушений

10.1.5. Предложения работников

10.2. Аудит и процедура обновления Политики

10.2.1. Внеплановые обновления Политики

10.2.2. Плановое обновление Политики

10.2.3. Оценка необходимости изменений

10.2.4. Разработка изменений

10.2.5. Утверждение изменений

10.3. Документирование и внедрение

10.3.1. Обновление документации

10.3.2. Обучение и информирование

Политики и стратегии

11.1. Политика информационной безопасности организации

11.2. Политика защиты персональных данных

11.3. Политика реагирования на компьютерные инциденты

11.4. Стратегия развития информационной безопасности

11.5. Стратегия защиты критической информационной инфраструктуры

Положения об отделе ИБ

12.1. Положение об отделе информационной безопасности

12.2. Положение о службе реагирования на инциденты информационной безопасности

Регламенты и инструкции

13.1. Инструкция по порядку учета и хранению съемных носителей конфиденциальной информации

13.2. Инструкция по обеспечению физической безопасности

13.3. Инструкция по использованию антивирусного ПО

13.4. Регламент проведения внутреннего аудита информационной безопасности

13.5. Регламент реагирования на компьютерные инциденты

Планы

14.1. План мероприятий по технической защите информации

14.2. План мероприятий по защите персональных данных

14.3. План внутренних проверок состояния защиты конфиденциальной информации

14.4. План мероприятий по переводу систем на отечественные средства защиты

Документы по контролю доступа

15.1. Инструкция по контролю доступа к информационным системам

15.2. Матрица доступа персонала к конфиденциальной информации

Конфигурационные файлы и технические настройки

16.1. Описание конфигурации и топологии АС (ИСПДн)

16.2. Технический паспорт объекта информатизации

16.3. Технический паспорт на защищаемое помещение

Документация по техническим средствам защиты

17.1. Перечень используемых сертифицированных технических средств защиты информации

Отчеты

18.1. Отчет по результатам аудита информационной безопасности

18.2. Отчет о проведенных учениях по противодействию компьютерным атакам

18.3. Отчет о состоянии защиты персональных данных

18.4. Отчет о состоянии защиты конфиденциальной информации

18.5. Отчет о результатах внутреннего аудита ИБ

18.6. Отчет о проведенных мероприятиях по технической защите информации

18.7. Отчет о результатах мониторинга защищенности информационных систем

18.8. Отчет о выявленных инцидентах информационной безопасности

18.9. Отчет о результатах расследования инцидентов ИБ

18.10. Отчет о результатах обучения сотрудников по вопросам ИБ

18.11. Отчет о результатах тестирования системы защиты информации

18.12. Отчет о состоянии **8. Отчеты** (продолжение) 18.14. Отчет о реализации мероприятий по переводу систем на отечественные средства защиты 18.15. Отчет о результатах анализа рисков ИБ 18.16. Отчет о реализации плана мероприятий по защите информации 18.17. Отчет о состоянии защищенности сетей и систем 18.18. Отчет о выполнении планов мероприятий по ИБ 18.19. Отчет о выполнении указаний ФСБ по ИБ 18.20. Отчет о проведенных проверках состояния защиты информации

1. **Оценки и анализы** 19.1. Оценка защищенности информационных систем 19.2. Анализ угроз безопасности информации
2. **Отчеты и уведомления** 20.1. Заключение о готовности СЗИ к эксплуатации 20.2. Копия уведомления об обработке персональных данных 20.3. Уведомление о проведении внутреннего аудита ИБ 20.4. Уведомление о планируемых проверках состояния защиты информации 20.5. Уведомление о выявленных инцидентах ИБ 20.6. Уведомление о результатах анализа рисков ИБ 20.7. Уведомление о результатах проверки состояния защиты информации 20.8. Уведомление о реализации мероприятий по защите информации
3. **Нормативно-правовые акты и методические материалы** 21.1. Нормативно-правовые акты по ИБ 21.2. Методические руководства по ИБ
4. **Регистры и журналы** 22.1. Журнал учета бумажных и съемных носителей конфиденциальной информации, в том числе ПДн 22.2. Журнал регистрации и учета обращений субъектов персональных данных
5. **Дополнительные документы** 23.1. Приказ о составе комиссии по классификации автоматизированных систем 23.2. Приказ о составе комиссии по классификации информационных систем персональных данных 23.3. Приказ о выделении помещения для обработки конфиденциальной информации 23.4. Приказ о назначении администраторов безопасности СЗ конфиденциальной информации 23.5. Приказ об утверждении мест хранения материальных носителей персональных данных 23.6. Приказ о назначении комиссии по уничтожению документов с ПД 23.7. Приказ на проектирование объекта информатизации 23.8. Приказ на проведение работ по защите информации 23.9. Приказ о назначении лиц, ответственных за эксплуатацию объекта информатизации 23.10. Приказ на обработку в АС конфиденциальной информации 23.11. Положение о порядке организации и проведения работ по защите конфиденциальной информации 23.12. Положение о порядке обработки и обеспечении безопасности персональных данных 23.13. Положение о подразделении по защите персональных данных 23.14. Положение о резервировании и восстановлении работоспособности ТС и ПО 23.15. Руководство пользователя по эксплуатации средств защиты конфиденциальной информации 23.16. Руководство администратора по эксплуатации средств защиты конфиденциальной информации 23.17. Руководство пользователя по обеспечению безопасности ИСПДн 23.18. Руководство администратора по обеспечению безопасности ИСПДн 23.19. Перечень сведений конфиденциального характера 23.20. Перечень АС и ИС, обрабатывающих конфиденциальную информацию 23.21. Перечень эксплуатационной и технической документации по средствам защиты информации 23.22. Перечень носителей персональных данных 23.23. Список помещений для обработки конфиденциальной информации 23.24. Утвержденный список лиц, допущенных в ЗП 23.25. Утвержденный список лиц, допущенных к работе на автоматизированных системах 23.26. Утвержденный список лиц, допущенных к персональным данным 23.27. Акт классификации АС 23.28. Акт классификации ИСПДн 23.29. Акт об уничтожении персональных данных субъекта 23.30. Модель угроз безопасности информации 23.31. Модель нарушителя 23.32. Частная модель угроз безопасности ПДн 23.33. План мероприятий по устранению недостатков в защите информации 23.34. Матрица доступа персонала к конфиденциальной информации 23.35. Ведомость приема зачетов по знанию законодательства по ИБ 23.36. Описание конфигурации и топологии АС (ИСПДн) 23.37. Условия расположения объекта информатизации относительно границы КЗ 23.38. Технический паспорт на защищаемое помещение 23.39. Письменное согласие субъектов персональных данных на обработку их ПДн

**Рекомендации по Оптимизации Документа:**

1. **Упрощение и Сжатие**: В каждом разделе включите только ключевые моменты, оставив подробности для приложений. Это поможет сосредоточиться на основных вопросах и сделать документ более удобным для использования.
2. **Использование Приложений**: Подробные инструкции и регламенты можно вынести в приложения. Это позволяет основному документу оставаться компактным, а пользователям — легко находить нужную информацию.
3. **Разделение по Роли и Процессам**: Разделите документ по ролям и процессам, чтобы каждая категория пользователей (например, руководство, IT-отдел, обычные сотрудники) могла легко найти соответствующую информацию.
4. **Интерактивные Элементы**: Если документ будет в электронном формате, добавьте интерактивные элементы (ссылки, закладки) для быстрого перехода между разделами и приложениями.
5. **Регулярные Обновления**: Определите регулярные промежутки времени для пересмотра и обновления документа, чтобы учитывать новые угрозы, изменения в законодательстве и технологические новшества.
6. **Обратная Связь и Корректировки**: Включите процесс обратной связи для пользователей политики, чтобы оперативно выявлять и исправлять неточности и недостатки.