Политика управления инцидентами информационной безопасности

# Общие положения

* 1. Настоящая политика определяет порядок управления инцидентами информационной безопасности в муниципальном учреждении.
  2. Политика распространяется на все информационные системы учреждения:

 систему автоматизированного управления транспортом;  базу персональных данных граждан;

 базу данных электронной приёмки граждан.

# Нормативные требования

Политика разработана с учётом требований следующих нормативных правовых актов:

 ФЗ-187 «О безопасности критической информационной инфраструктуры РФ»;  ФЗ-152 «О персональных данных»;

 приказа ФСТЭК России № 21;  приказа ФСБ России № 766.

# Термины и определения

* 1. **Инцидент ИБ** - событие, которое может привести к нарушению безопасности информации.
  2. **Система управления инцидентами** - комплекс мероприятий по обнаружению, анализу и реагированию на инциденты.

# Схема процесса управления инцидентами

Этапы процесса:

обнаружение инцидента; классификация и оценка; реагирование и локализация; расследование и анализ; восстановление;

документирование и отчетность

# Распределение ответственности

Ответственные лица:

 **Руководитель отдела ИБ** - общее руководство процессом;

 **Системный администратор** - оперативное реагирование и техническая поддержка;

 **Специалисты по ИБ отделов** - реагирование в своей зоне ответственности;

 **Операторы систем** - первичное обнаружение;

 **Комиссия по ИБ** - расследование инцидентов.

# Действия участников процесса

При обнаружении инцидента:

немедленное уведомление системного администратора; сохранение всех логов и доказательств;

отключение системы при необходимости; уведомление руководителя отдела ИБ.

При реагировании:

оценка критичности инцидента; локализация угрозы; уведомление руководства;

при необходимости - уведомление регуляторов (РосКомНадзор, ФСБ).

После локализации:

 расследование причин;  анализ последствий;

 восстановление систем;

 подготовка отчета о произошедшем инциденте.

# Организационно-распорядительная документация

Перечень ОРД:

регламент управления инцидентами; инструкции по реагированию; формы отчётности;

 журналы регистрации инцидентов;

 шаблоны уведомлений регуляторов.

# Должностные инструкции

## Системный администратор:

мониторинг систем защиты; реагирование на инциденты;

координация действий при инциденте; анализ инцидентов;

техническая поддержка; восстановление систем; резервное копирование.

## Руководитель отдела ИБ:

координация процесса управления инцидентами; принятие решений по реагированию;

контроль выполнения процедур; взаимодействие с регуляторами.

## Специалисты по ИБ отделов:

 реагирование на инциденты в своей зоне ответственности;  участие в расследовании;

 восстановление систем.

# Дополнительные документы

План реагирования на инциденты:

сценарии действий; контакты ответственных лиц;

порядок восстановления систем;

сроки хранения данных.

процедуры уведомления регуляторов.

Журнал регистрации инцидентов:

форма фиксации инцидентов; порядок ведения журнала;

# Контроль и отчётность

Ежемесячная отчётность:

статистика инцидентов; анализ эффективности мер; рекомендации по улучшению;

отчёты о уведомлениях регуляторов.

Квартальный анализ:

 оценка рисков;

 корректировка процедур;  обучение персонала.

# Заключительные положения

* 1. Политика вступает в силу с момента утверждения.
  2. Изменения вносятся решением руководства учреждения.
  3. Контроль исполнения возлагается на руководителя службы ИБ.
  4. Все изменения и дополнения к политике должны учитывать требования нормативных правовых актов и проходить согласование с соответствующими структурами.