Приложение №2

к Положению о физической безопасности

при осуществлении ядерной и

радиологической деятельности

**Типовое содержание Плана физической безопасности**

План физической безопасности должен содержать информацию, необходимую для описания мер безопасности и системы физической безопасности, а также быть соизмеримым с категорией источника и объектом. Предусмотренные меры должны учитывать и аспект кибербезопасности как неотъемлемую часть физической безопасности, которая должна органически сочетаться с другими компонентами физической безопасности, а также предусматривать влияние на правовые ресурсы, персонал и технические ресурсы системы. Должны быть представлены следующие субъекты:

1) описание ядерного и радиоактивного материала, категория и использование;

2) описание окружающей среды, сооружения и/или установки, где используется или хранится источник, схема размещения и системы безопасности, при необходимости;

3) размещение сооружения или установки по отношению к зоне общественного доступа;

4) анализ риска несанкционированного проникновения на ядерный и радиологический объект;

5) внутренние процедуры обеспечения безопасности;

6) цели плана безопасности сооружений и установок, включая:

а) предотвращение несанкционированного хищения, уничтожения или злонамеренного использования;

b) необходимый контроль для предотвращения негативных последствий, в том числе возможность оснащения необходимым дополнительным оборудованием;

с) установки или объекты, подлежащие защите;

7) меры по обеспечению безопасности, которые будут применяться, в том числе:

а) по предупреждению, обеспечению мониторинга, контролю доступа, обнаружению, удержанию, реагированию и связи;

b) конструктивные особенности (для оценки мер, направленных против угрозы);

8) административные меры, которые будут использованы, включают:

а) роль безопасности и ответственности администрации, персонала и других лиц;

b) обычные меры или свободные меры, в том числе учет источников;

с) техническое обслуживание и тестирование оборудования;

d) оценка уровня подготовки персонала;

е) внедрение информационной безопасности;

f) методы санкционированного доступа;

g) план реагирования при чрезвычайных ситуациях;

h) обучение;

9) соответствие угрозы определенному уровню физической безопасности;

10) процедуры регулярной оценки эффективности плана и его периодическое обновление.