

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ
ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ УСТАНОВОК**

Сайидкомил Ибодуллаев

Преподаватель кафедры «Международное частное право»
Ташкентского государственного юридического университета
siresearchuz@gmail.com<https://doi.org/10.5281/zenodo.16949290>**Введение**

Физическая защита ядерных установок (далее — ФЗЯУ) является ключевым элементом национальной ядерной безопасности и важнейшим компонентом международного режима ядерной безопасности. Под данным термином в международно-правовом и национальном контексте понимается комплекс организационных, правовых, технических и инженерных мер, направленных на предотвращение несанкционированного доступа, диверсий, кражи ядерного материала, а также любых действий, способных вызвать радиационные последствия для здоровья населения и окружающей среды.

В последние два десятилетия глобальная обстановка, связанная с угрозами ядерного терроризма и диверсий, существенно усложнилась. Ключевым толчком для реформирования международных и национальных правовых механизмов стала, в частности, серия событий начала XXI века: террористические атаки 11 сентября 2001 года, которые привели к пересмотру подходов к охране критически важной инфраструктуры, включая объекты атомной энергетики, а также инциденты в ряде государств, когда на территории ядерных установок фиксировались попытки незаконного проникновения.

На международном уровне основу правового регулирования ФЗЯУ составляет **Конвенция о физической защите ядерного материала** (Вена, 1980 г., далее — КФЗЯМ) и **Поправка к ней 2005 года**, вступившая в силу в мае 2016 года. Поправка существенно расширила сферу действия Конвенции, распространив обязательства государств не только на международную перевозку ядерного материала, но и на его защиту при внутреннем использовании, хранении и транспортировке. Дополнительную правовую рамку составляют документы МАГАТЭ, в частности, **INFCIRC/225/Rev.5 — «Физическая защита ядерного материала и ядерных установок»**, а также Серия рекомендаций по физической защите (Nuclear Security Series, NSS).

Вместе с тем, несмотря на наличие развитой международной нормативной базы, практика применения этих стандартов в национальных правовых системах выявляет целый ряд актуальных проблем, включая разрыв между обязательными нормами и рекомендациями, различие в технических стандартах, недостаточную подготовку персонала, а также вопросы правоприменения и ответственности за нарушения в сфере физической защиты.

Международно-правовые стандарты и их имплементация в национальное законодательство

Система международных норм по физической защите ядерных установок строится на комплексном сочетании договорных обязательств, мягкого права (soft law) и рекомендаций технического характера.

Ключевым универсальным инструментом является **Конвенция о физической защите ядерного материала (КФЗЯМ)**, принятая в 1980 г. и дополненная Поправкой 2005 г. Поправка существенно расширила сферу применения Конвенции, закрепив, что государства-участники обязаны разрабатывать, внедрять и поддерживать на национальном уровне режим физической защиты, охватывающий:

- эксплуатацию ядерных установок;
- хранение и транспортировку ядерного материала;
- предотвращение и пресечение актов незаконного вмешательства.

В дополнение к этому, международные стандарты МАГАТЭ, прежде всего **INFCIRC/225/Rev.5**, содержат систематизированные рекомендации по проектированию, внедрению и оценке систем физической защиты. Этот документ отражает принципы *глубокошелонированной защиты* (defence-in-depth), интеграцию мер охраны с инженерными и технологическими решениями, а также применение риск-ориентированного подхода.

Особое значение имеют рекомендации **Серии по ядерной безопасности МАГАТЭ (Nuclear Security Series, NSS)**, где рассматриваются как общие принципы защиты, так и специализированные руководства для конкретных типов объектов — от исследовательских реакторов до установок по переработке отработанного топлива.

Однако имплементация этих стандартов в национальное законодательство неоднородна. В **США** регулирование базируется на положениях **Atomic Energy Act (1954)** и нормативных актах **Nuclear Regulatory Commission (NRC)**, где установлены обязательные лицензионные требования по физической защите, инспекционным проверкам и подготовке персонала. В **Европейском Союзе** вопросы физической защиты интегрированы в законодательство Евратома и гармонизированы с национальными правовыми актами через директивы и технические стандарты, например **Council Directive 2009/71/Euratom** с поправками 2014 года.

В **Российской Федерации** основу правового регулирования составляют **Федеральный закон «Об использовании атомной энергии»** и подзаконные акты, включая **Правила физической защиты ядерных установок и ядерных материалов** (утв. Ростехнадзором).

В **Узбекистане** процесс формирования системы ФЗЯУ находится в активной стадии. Принятый в 2019 г. **Закон «Об использовании атомной энергии в мирных целях»** закрепляет общие требования к физической защите, отсылая к нормативным документам МАГАТЭ. Важную роль играет также межведомственная координация — между Госкоматомом, Министерством внутренних дел и Службой государственной безопасности. При этом в практике выявляются пробелы, связанные с отсутствием детализированных национальных стандартов, эквивалентных INFCIRC/225, и недостаточным уровнем подготовки охранного персонала по международным методикам.

Актуальные проблемы правоприменения в сфере физической защиты ядерных установок

Современная практика правоприменения в области ФЗЯУ сталкивается с целым рядом вызовов, которые имеют как техническое, так и правовое измерение.

1. Технологическое устаревание систем охраны

Многие действующие ядерные установки, особенно в странах с длительным опытом эксплуатации атомной энергетики, были введены в строй в 1970–1980-х гг. Их первоначальные системы физической защиты, как правило, разрабатывались в соответствии с технологическими возможностями того времени и не отвечают современным требованиям МАГАТЭ. Это касается как инженерно-технических средств (датчиков, видеонаблюдения, систем контроля доступа), так и программного обеспечения. Замена или модернизация таких систем требует значительных инвестиций и, как показывает практика ряда стран, нередко сопровождается правовыми спорами относительно распределения расходов между оператором, государством и подрядчиками.

2. Внутренние угрозы (Insider Threat)

Международный опыт (в частности, расследования в США, Южной Корее и Южной Африке) показал, что значительную опасность для ядерных объектов представляют несанкционированные действия сотрудников с легальным доступом. INFCIRC/225/Rev.5 прямо предписывает государствам учитывать данный фактор при разработке режимов ФЗЯУ. Однако в ряде национальных правовых актов отсутствуют чёткие процедуры психологического отбора, периодической проверки благонадёжности персонала и обязательного обмена информацией между работодателем и правоохранительными органами.

3. Киберугрозы и интеграция ИТ-защиты

Современные ядерные установки являются сложными киберфизическими системами, управление которыми осуществляется с применением автоматизированных систем управления технологическими процессами (АСУ ТП). Взлом или саботаж таких систем может привести к катастрофическим последствиям. Международные рекомендации МАГАТЭ (NSS No. 17) призывают интегрировать меры киберзащиты в общую систему физической защиты. Тем не менее, анализ национальных нормативов в ряде стран, включая государства Центральной Азии, показывает, что киберугрозы зачастую рассматриваются отдельно от физической защиты, что создаёт нормативные пробелы.

4. Взаимодействие с международными инспекционными миссиями

МАГАТЭ в рамках программ IPPAS (International Physical Protection Advisory Service) и INSServ (International Nuclear Security Advisory Service) проводит инспекции и консультативные визиты, оценивая соответствие национальных режимов ФЗЯУ международным стандартам. В некоторых случаях рекомендации этих миссий не находят своевременного отражения в национальном законодательстве из-за отсутствия чётких процедур имплементации и межведомственной координации.

5. Проблема баланса между прозрачностью и конфиденциальностью

Правоприменительная практика сталкивается с дилеммой: обеспечение общественного контроля за безопасностью ядерных объектов требует определённого уровня прозрачности, однако чрезмерное раскрытие информации о системах охраны может создать дополнительные уязвимости. Национальные законы об информации и государственные стандарты по защите сведений не всегда содержат сбалансированные

положения, что может приводить либо к неоправданной секретности, либо, напротив, к рисковому разглашению деталей.

Заключение и рекомендации

Анализ международных и национальных подходов к правовому регулированию физической защиты ядерных установок показывает, что успешное функционирование системы ФЗЯУ возможно только при комплексном учёте технических, организационных и правовых факторов.

1. Усиление нормативной базы

Необходимо разработать и внедрить в национальное законодательство специализированные подзаконные акты, детализирующие требования по проектированию, эксплуатации и модернизации систем физической защиты. Эти документы должны учитывать положения INFCIRC/225/Rev.5, NSS МАГАТЭ, а также адаптировать международный опыт, например, модели NRC (США) и Euratom (ЕС).

2. Интеграция киберзащиты в общую систему ФЗЯУ

Рекомендуется законодательно закрепить обязанность операторов ядерных установок внедрять меры информационной и кибербезопасности в составе общей системы физической защиты. В этом контексте целесообразно опираться на стандарты МАГАТЭ (NSS No. 17) и руководящие документы МЭК (IEC 62645).

3. Развитие механизмов противодействия внутренним угрозам

Следует предусмотреть обязательное лицензирование и периодическую переаттестацию охранного персонала, многоступенчатые процедуры проверки благонадёжности (background check), а также правовое регулирование обмена информацией между правоохранительными органами и операторами.

4. Институционализация взаимодействия с МАГАТЭ

Для эффективного внедрения рекомендаций IPPAS и INSServ необходимо закрепить в законе обязательность рассмотрения их итоговых отчётов на межведомственном уровне с последующей разработкой «дорожных карт» по реализации предложений.

5. Оптимизация баланса между прозрачностью и секретностью

В законе об информации и в актах о государственной тайне следует чётко определить перечень сведений, подлежащих обязательному раскрытию в целях общественного контроля (например, общие показатели готовности к ЧС), и категорий данных, которые подлежат строгой защите (например, технические параметры охранных систем).

References:

Используемая литература:

Foydalanilgan adabiyotlar:

1. Convention on the Physical Protection of Nuclear Material (CPPNM), IAEA, 1980; Amendment of 2005.
2. IAEA Nuclear Security Series No. 13 (INFCIRC/225/Rev.5), *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, IAEA, 2011.
3. IAEA Nuclear Security Series No. 17, *Computer Security at Nuclear Facilities*, IAEA, Vienna,

2016.

4. Atomic Energy Act of 1954, as amended, United States Code, Title 42, Chapter 23.
5. Council Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations, OJ L 172, 2.7.2009.
6. Федеральный закон Российской Федерации от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии».
7. Закон Республики Узбекистан от 09.09.2019 № ЗРУ-562 «Об использовании атомной энергии в мирных целях».
8. IEC 62645:2019, *Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based systems*.
9. International Physical Protection Advisory Service (IPPAS) Guidelines, IAEA, Vienna, 2020.
10. World Nuclear Association, *Security of Nuclear Facilities and Materials*, updated 2024.