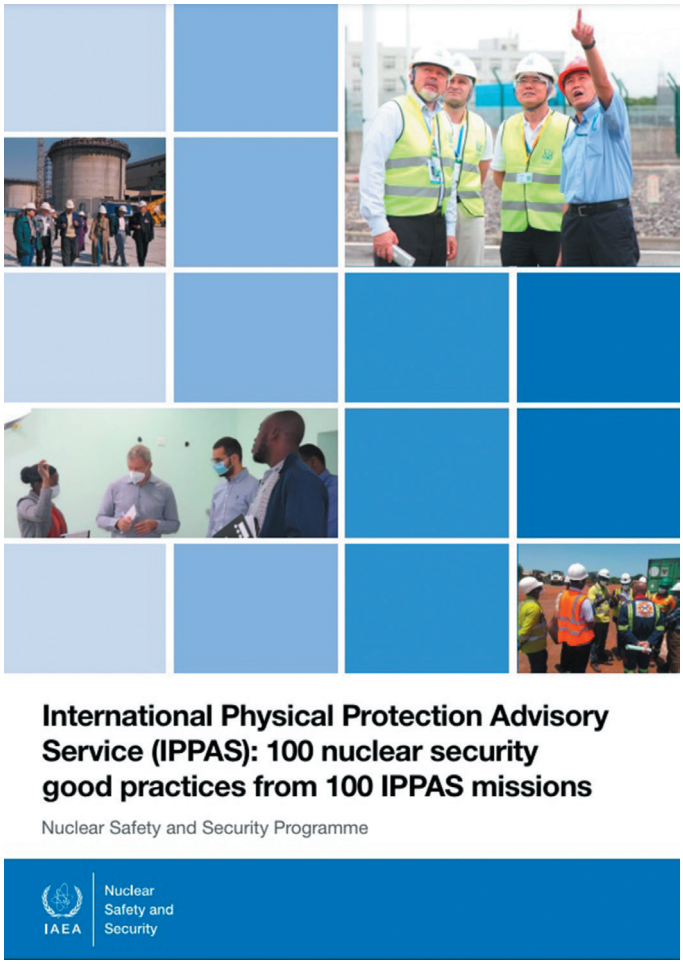
## МЕЖДУНАРОДНАЯ ИНФОРМАЦИЯ

# Сто миссий МАГАТЭ (IPPAS) – «100 лучших практик» в области физической ядерной безопасности

Крупчатников Б. Н., консультант научно-организационного отдела ФБУ «НТЦ ЯРБ» (krupchatnikov@secnrs.ru),
Гареев М. Д., начальник отдела учета, контроля, физической защиты ядерных материалов и радиоактивных веществ ФБУ «НТЦ ЯРБ» (gareev@secnrs.ru)




МАГАТЭ опубликовало информацию о 100 проведенных миссиях Международной консультативной службы по физической защите (International Physical Protection Advisory Service – IPPAS) (далее – Миссия), в которой представлены «100 лучших практик» в области физической ядерной безопасности[1]. Отмечается, что, с момента зарождения в 1995 г. этой консультативной услуги МАГАТЭ, ею воспользовались 60 государств-членов, которые приняли у себя 100 миссий IPPAS.

Подчеркивается, что, в связи с изменением видов угроз физической ядерной безопасности в сферу деятельности IPPAS, включен модуль по анализу информационной и компьютерной безопасности в контексте физической защиты, и создана база данных о передовой практике IPPAS в этом направлении[2].

[1] International Physical Protection Advisory Service (IPPAS): 100 nuclear security good practices from 100 IPPAS missions. [Электронный ресурс]. URL: https://www.iaea.org/sites/default/files/23/09/international-physical-protection-advisory-service-ippas-100-nuclear-security-good-practices-from-100-ippas-missions.pdf (дата обращения: 10.06.2024).

[2] МАГАТЭ ведет базу данных передовой практики IPPAS с 2016 г., чтобы делиться результатами таких миссий с международным сообществом по ядерной безопасности. Ведение базы данных и обмен примерами по конфиденциальности помогают IPPAS увеличить отдачу от помощи, предлагаемой МАГАТЭ своим государствам-членам. В настоящее время база данных включает 532 примера передового опыта, что является результатом 90 миссий IPPAS, проведенных до конца 2019 г. База данных доступна для назначенных контактных лиц государств-членов.

В настоящее время Миссия реализует модульный подход, который позволяет адаптировать ее цели к запросам принимающего государства. Существует пять модулей:

Модуль 1 – Национальный режим физической ядерной безопасности ядерных материалов и ядерных установок;

Модуль 2 – Физическая ядерная безопасность ядерной установки;

Модуль 3 – Физическая безопасность при транспортировании;

Модуль 4 – Безопасность радиоактивных материалов, связанных с ними установок и деятельности;

Модуль 5 – Информационная и компьютерная безопасность.

В настоящее время разрабатывается шестой модуль, который будет включать вопросы учета и контроля ядерных материалов в целях обеспечения физической ядерной безопасности.

В публикации указывается, что Миссия позволяет осуществлять конфиденциальный обмен опытом и передовыми практиками. Повестка дня включает обсуждения с экспертами и официальными лицами принимающей страны, посещение объектов, наблюдение, а также обзор национального законодательства и опыта регулирования. Миссия предоставляет государствам-членам рекомендации по выполнению международных обязательств, принятых Конвенцией по физической защите ядерного материала и ядерных установок и Резолюцией 1540 Совета Безопасности Организации Объединенных Наций о противодействии ядерному терроризму. В ходе Миссии группа экспертов рассматривает деятельность государств-членов в области физической защиты ядерных и других радиоактивных материалов, связанных с ними объектов использования атомной энергии и деятельности, в соответствии с рекомендациями МАГАТЭ по физической ядерной безопасности, содержащимися в документах серии «Физическая ядерная безопасность» (Nuclear Security Series – NSS).

Некоторые из примеров «Ста лучших практик» приведены ниже с обобщением содержания рекомендаций каждого модуля. Большинство из них реализованы в российской практике и являются обязательными мерами физической защиты. Другие, касающиеся, например, модуля 5 «Информационная и компьютерная безопасность», могут представлять интерес для лицензиата, регулятора, сил охраны и иных лиц, деятельность которых так или иначе связана с физической защитой.

## Модуль 1 – Национальный режим физической ядерной безопасности ядерных материалов и ядерных установок

***Подраздел «Стратегия, политика и культура физической ядерной безопасности»:***

- наличие политики в области культуры физической ядерной безопасности на государственном уровне в гражданском секторе атомной промышленности;
- регулярное проведение семинаров и круглых столов для развития культуры физической ядерной безопасности;
- проведение оператором самооценки состояния культуры физической ядерной безопасности в организации и направление результатов регулятору;
- создание координационного органа/совета по физической ядерной безопасности с участием представителей всех вовлеченных ведомств для рассмотрения и консультирования по стратегическим вопросам физической ядерной безопасности межведомственного уровня, обеспечение координации и сотрудничества между соответствующими органами власти и организациями;
- наличие национального центра по культуре физической ядерной безопасности, наличие меморандумов и соглашений о взаимопонимании и о сотрудничестве, устанавливающих конкретные роли и обязанности организаций, участвующих в физической защите и устанавливающих процедуры и процессы для обеспечения эффективного взаимодействия между этими сторонами;
- отнесение вопросов эксплуатационной безопасности, физической ядерной безопасности и гарантий в ведение одной регулирующей организации, что способствует их синергии, а также участию на постоянной основе заинтересованных сторон в процессе выработки регулирующих правил с целью сделать их более приемлемыми и эффективными;
- наличие резидент-инспекторов для обеспечения постоянного надзора на энергетических реакторах и радиационных установках с источниками категории I.

***Подраздел «Оценка угроз и разработка проектной угрозы (Design Basis Threat – DBT), планы действий в чрезвычайных ситуациях, готовность и реагирование»:***

- создание организационной структуры, включающей информационные и компьютеризованные каналы передачи экстренной информации;
- обучение и информирование сил реагирования, разработка для них, а также для оператора установки четких и кратких инструкций на случай инцидента физической ядерной безопасности;
- регулярное обновление планов действий в чрезвычайных ситуациях и проведение соответствующих учений на национальном уровне.

**Модуль 2 – Физическая ядерная безопасность ядерной установки:**

- дифференцированный подход при проверке благонадежности персонала и установлении прав доступа в зоны безопасности (защищенные зоны);
- тесное взаимодействие оперативного персонала и службы безопасности, взаимное ознакомление сотрудников с вопросами безопасности и физической ядерной безопасности, наличие четких и кратких инструкций на случай возникновения событий физической ядерной безопасности;
- использование современных тренажеров пунктов управления в системе физической защиты для обучения сотрудников сил реагирования, меры по удержанию квалифицированного персонала физической защиты;
- наличие программ технического обслуживания средств физической защиты, интегрированных в общую систему обеспечения качества, включая профилактическое и корректирующее обслуживание, а также проверки в процессе эксплуатации и периодические испытания с теми же строгими режимами, что и для систем эксплуатационной безопасности;
- повышение культуры физической безопасности путем разработки интерфейса оперативного персонала и персонала службы безопасности.

**Модуль 3 – Физическая безопасность при транспортировании:**

- участие на постоянной основе водителя транспортного средства в обеспечении безопасности перевозимых источников в дополнение к лицу, сопровождающему груз;
- наличие центра транспортного контроля, позволяющего отслеживать местоположение транспортных средств в режиме реального времени, обеспечивающего эффективное реагирование на инциденты, связанные с физической ядерной безопасностью;
- участие оперативного центра по чрезвычайным ситуациям с его каналами связи и ролью в координации действий всех заинтересованных сторон, позволяющего осуществлять эффективный, защищенный обмен информацией, связанной с безопасностью во время транспортировки ядерного материала.

**Модуль 4 – Безопасность радиоактивных материалов, связанных с ними установок и деятельности:**

- вопросы организации сотрудничества как на международном уровне, так и на межведомственном, с участием правоохранительных организаций, в том числе обмен информацией, улучшающей понимание существующих в мире угроз;
- поддержание уровня квалификации персонала, участвующего в обеспечении физической безопасности источников, и осведомленности по вопросам радиационной защиты сил реагирования, создание магистерских программ по физической ядерной безопасности, проведение семинаров, учений, в том числе незаявленных, на таможенных пунктах пропуска;
- оценка экспортером рисков физической безопасности источников у получателя;
- усиление мер контроля при перемещении и транспортировании источников, мер контроля доступа, в особенности портативных и высокоактивных радиационных источников, используя системы видеонаблюдения, правило двух лиц и систему двухфакторной идентификации;
- использование скрытых устройств типа тревожной кнопки, обеспечивающих немедленное оповещение персонала службы безопасности о вторжении или принуждении к незаконным действиям.

**Модуль 5 – Информационная и компьютерная безопасность:**

- предоставление ресурсов для поддержки операторов установок и органов власти национального уровня, обладающих специализированными возможностями и полномочиями в области компьютерной безопасности;
- создание специального управления по компьютерной безопасности для планирования, координации и управления деятельностью компетентного органа в области компьютерной и информационной безопасности, включая группу оценки кибербезопасности для мониторинга угроз;
- регулярное осуществление межведомственного обмена информацией о развитии компьютерных угроз и уязвимостей со стороны компетентного органа;
- применение подхода, ориентированного на достижение конечного результата, основанного на проектной киберугрозе, отражение этого подхода в руководствах по ИТ-безопасности, обеспечивающих гибкую основу для предотвращения кибератак и защиты от них ядерных установок;
- наличие единой концепции компьютерной безопасности для всех жизненно важных секторов, ее реализация под руководством единого компетентного органа;
- анализ информации о реальных и потенциальных событиях в мире в энергетическом секторе, включая ядерные объекты, предоставление ее соответствующим органам и операторам установок;
- создание совета по компьютерной безопасности национального уровня, состоящего из представителей различных ведомств, научных кругов, государственного и частного секторов, с целью обмена информацией между соответствующими заинтересованными сторонами;
- контроль вывоза с объекта компьютерного оборудования и любых информационных ресурсов;
- участие группы компьютерной безопасности во всех мероприятиях по закупке и вводу в эксплуатацию средств физической защиты и средств защиты цифровых активов, важных для безопасности;
- внедрение специализированных защищенных портативных носителей для передачи данных в автономных сетевых средах и за их пределами, обеспечение строгого контроля потенциальной миграции вредоносных программ;
- создание центра мониторинга компьютерной безопасности для сбора информации из различных сетей и доменов и оказания помощи в раннем обнаружении аномалий или попыток вторжения;
- наличие на площадке АЭС специальной тестовой среды, которая отражает целевую цифровую среду объекта и позволяет проводить эффективное тестирование компьютерной безопасности без ущерба для безопасности действующих систем объекта;
- изоляция операционной и автоматизированной сети от внешнего трафика для защиты от вредоносных программ;
- отсутствие негативного влияния на меры эксплуатационной и физической безопасности и функционирование объекта при разработке компьютерной безопасности;
- проведение оценки угрозы для каждого нового актива и определение соответствующих характеристик и мер защиты перед размещением в сети объекта с целью обеспечения минимальной уязвимости в случае атаки;
- создание на объекте группы компьютерной безопасности, установление для нее процедур, ролей и обязанностей, правил коммуникации с дежурным персоналом, сотрудничество группы с внешними организациями, отвечающими за кибербезопасность.