# 4. ОПРЕДЕЛЕНИЕ ПОТЕНЦИАЛЬНЫХ УГРОЗ И СПОСОБОВ ИХ РЕАЛИЗАЦИИ

## 4.1. Угрозы безопасности объекта

Наличие на объекте ядерных материалов приводит к появлению серьезных дополнительных специфических угроз безопасности ЯОО и естественным образом определяет повышенные требования к защищенности ЯОО (рисунок 19). Предотвращение реализации именно этих угроз и является основной ***целью и задачей систем физической защиты ЯОО***.

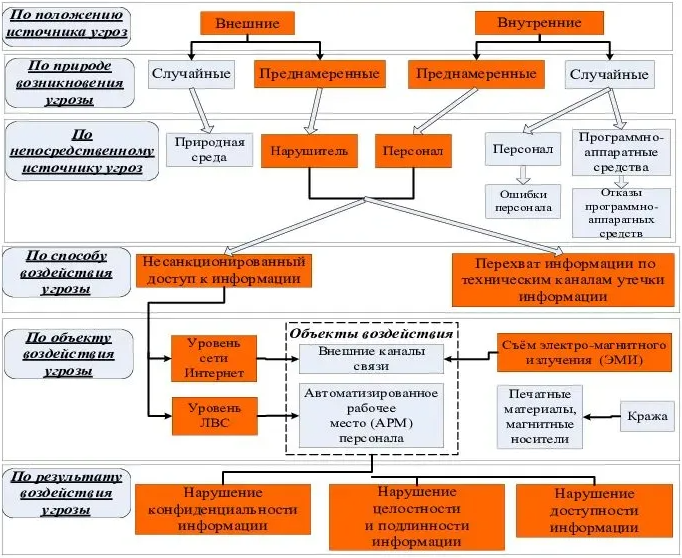


Рисунок 19. Классификация угроз безопасности ядерно-опасного объекта.

В виду того, что неправильное обращение с ЯМ, вмешательство в работу ядерных энергетических устройств (ЯЭУ) или нарушение технологических процессов с ЯМ может привести к очень серьезным последствиям, связанным с угрозой жизни и здоровью большого количества людей и экологической катастрофе, ЯОО становятся привлекательной целью для различных экстремистских и террористических организаций или просто психически неуравновешенных людей. Тот же самый результат можно получить несанкционированным вмешательством (может даже непреднамеренным) неквалифицированного сотрудника ЯОО в некий технологический процесс, следовательно, на территории ЯОО должна четко и бесперебойно действовать система контроля и управления доступом, система обнаружения и т.д. Кроме того, ЯМ являются необходимым сырьем для производства ядерного оружия, которое для достижения своих политических целей хотели бы иметь многие страны третьего мира и международные террористические организации. Однако организация процесса производства ЯМ, готовых к применению в ядерном оружии, требует реализации сложных наукоемких технологий, больших экономических затрат и кроме того, это не пройдет не замечено для других стран. Поэтому возможность спланированного и организованного кем-то нападения на ЯОО, с целью хищения уже готовых ЯМ, представляет определенную угрозу. Также хищение ЯМ может производиться сотрудниками ЯОО для продажи с целью обогащения.

***Основными угрозами безопасности ЯОО являются***:

* вооруженное нападение на ЯОО;
* тайное проникновение нарушителей на ЯОО или его отдельные зоны;
* организация диверсий и террористических актов на ЯОО;
* хищение ЯМ;
* подкуп или шантаж сотрудников ЯОО для получения их помощи в хищении ЯМ или проникновении на ЯОО.

Таким образом, функционирование СФЗ ЯОО направлено на предотвращение проникновения нарушителей на ЯОО, хищений ЯМ, а также несанкционированных действий в отношении ЯМ, ядерно-опасных изделий, установок или транспортных средств, перевозящих ЯМ.

При составлении списка возможных угроз реальному ЯОО особую проблему, связанную с тем, что количество уже имевших место серьезных случаев преступных или враждебных действий на атомных объектах относительно невелико, представляет сбор необходимой информации. В данном случае необходимо накопить как можно больше информации, поступающей из различных источников.

Условия местной среды позволяют получить информацию об опасности, угрожающей тому или иному индивидуальному объекту. Следует учитывать как условия, существующие за пределами объекта, так и характеристики самого объекта. Внешние условия, например, общие настроения населения окружающего объект района, характер окружающей местности (густонаселенный, городской или малонаселенный, сельский), а также наличие в окружающем объект районе определенных организованных групп, могут послужить источником информации о существующей угрозе. Условия на территории самого объекта, такие, как состав рабочей силы, характер трудовых отношений, правила взаимодействия с другими предприятиями, принципы взаимоотношений с представителями общественности, сознательность в том, что относится к обеспечению безопасности и охране объекта, наличие программ проверки и повышения надежности персонала, могут повлиять на характеристики возможной угрозы.

Изучение и определение характеристик местного и общенационального состава населения могут быть полезны при определении возможной угрозы определенному атомному объекту. Любая неудовлетворенная или враждебно настроенная существенная фракция населения должна быть изучена отдельно. При изучении такой фракции населения особое внимание следует уделять имеющим боевой опыт ветеранам вооруженных сил, опытным техническим специалистам, политическим экстремистам и людям, имевшим ранее доступ на территорию атомных объектов.

Можно указать некоторые характеристики объекта, более или менее привлекательные для нарушителя, который стремится использовать их в свою пользу. К ним относятся географические или конструкционные особенности объекта, привлекательность находящихся на территории объекта определенных целей, представление диверсанта об эффективности системы физической защиты.

## 4.2. Виды угроз

***К потенциальным угрозам в отношении объекта относятся:***

а) ***угроза захвата*** – возможность захвата объекта, установления над ним контроля силой или угрозой применения силы, или путем любой другой формы запугивания;

б) ***угроза взрыва (разрушения)*** – возможность разрушения объекта или нанесения ему, здоровью персонала и другим лицам повреждений путем взрыва (затопления);

в) ***угроза*** ***размещения или попытки размещения на объекте взрывных устройств (взрывчатых веществ)*** – возможность размещения или совершения действий в целях размещения каким бы то ни было способом на объекте взрывных устройств (взрывчатых веществ), которые могут разрушить объект, нанести ему повреждения;

г) ***угроза поражения опасными веществами*** – возможность загрязнения объекта опасными химическими, радиоактивными или биологическими агентами, угрожающими жизни или здоровью персонала и других лиц;

д) ***угроза блокирования*** – возможность создания препятствия, ограничивающего функционирование объекта, угрожающего жизни или здоровью персонала и других лиц;

е) ***угроза хищения*** – возможность совершения хищения элементов объекта, которое может привести к нарушению технологического процесса, влекущему аварию на объекте с угрозой жизни и здоровью персонала и других лиц, а также возникновению чрезвычайных ситуаций с опасными социально-экономическими последствиями;

ж) ***угроза технического воздействия*** – несанкционированные действия техническими способами в отношении систем электропитания, управления или защиты технологических процессов (включая дистанционные) объекта с целью вывода их из строя, а также хищение секретной или конфиденциальной информации, использование которой может облегчить организацию несанкционированных действий в отношении объекта.

## 4.3. Основные источники угроз ЯО

Под угрозами ядерно-опасным объектам понимаются потенциальные возможности хищений ядерных материалов и совершения диверсий в отношении ядерных материалов и пунктов их хранения.

Основными источниками угроз ядерно-опасным объектам являются (в общем виде):

* отказы и неисправности оборудования ядерных установок (ЯУ), пунктов хранения ядерных материалов (ЯМ), другого жизненно важного для ядерно опасного оббъекта (ЯОО) оборудования;
* непрофессиональные или умышленные действия человека.

По отношению к ЯОО ***источники угроз*** могут быть разделены на ***внешние, внутренние и комбинированные***.

**Внешние** угрозы исходят от лиц, не входящих в состав персонала ЯОО и не имеющих права доступа на территорию ЯОО. Внешние угрозы реализуются внешним нарушителем.

**Внутренние** угрозы исходят от персонала ЯОО и других лиц, допущенных в охраняемые зоны объекта. Внутренние угрозы реализуются внутренним нарушителем.

**Комбинированные** угрозы исходят одновременно от внешних и внутренних нарушителей, действующих совместно (в сговоре).

В общем случае следует предполагать, что нарушители, как внешние, так и внутренние, обладают высокой степенью информированности об особенностях ЯОО и СФЗ.

Исходя из целей проведения анализа уязвимости ЯОО в Методических рекомендациях рассматриваются только те вероятные способы осуществления угроз ЯОО, с помощью которых реализуются возможности внешних и внутренних нарушителей по совершению хищений ЯМ, диверсий в отношении ЯМ, ЯУ и пунктов хранения ЯМ.

К вероятным способам осуществления угроз ЯОО со стороны внешних нарушителей можно отнести следующие:

* нападение и проникновение на ЯОО группы террористов с использованием любых возможных транспортных средств, оружия, взрывчатых и зажигательных веществ;
* проникновение группы (толпы) экстремистски настроенных противников атомной энергетики или других видов ядерной деятельности (антиядерных экстремистов) с целью занять ЯУ и совершить несанкционированные действия в связи с выдвижением политических, экономических или экологических требований;
* повреждение ими жизненно важных для ЯОО сооружений и оборудования, расположенных за пределами защищённой зоны, способное привести к опасным радиационным последствиям;
* дистанционный вывод из строя различных электронных систем и систем связи.

К вероятным способам осуществления угроз ЯОО со стороны внутренних нарушителей можно отнести следующие:

* хищение ЯМ;
* рассеяние ЯМ, в том числе, с помощью взрыва;
* повреждение персоналом ЯОО оборудования, устройств или какого-либо их элемента, способное привести к опасным радиационным последствиям;
* вмешательство в работу вычислительной техники, участвующей в управлении работой ЯУ, или инженерно-технических средств, входящих в состав СФЗ;
* вывод из строя или изменение заданных параметров используемых технических средств СФЗ любыми доступными способами;
* воздействие на технические средства.

Вышеприведённые перечни воздействий не являются исчерпывающими, они могут дополняться исходя из специфики конкретного ЯОО и особенностей его территориального расположения.

Внутренние нарушители опасны также тем, что они имеют высокую профессиональную квалификацию, могут обладать не только знанием уязвимых мест ЯУ и СФЗ, но и имеют право доступа к ним и к соответствующей информации.

Кроме этого, растущая автоматизация производственных процессов и применение цифровых технологий при эксплуатации ядерных установок и обращении с радиоактивными материалами увеличивают риск нападения на автоматизированные системы (АС) с использованием программно-технических средств и телекоммуникационных сетей. Иначе говоря, создают риск кибератак.

Обеспечение кибербезопасности — проблема, актуальная для всех объектов критической инфраструктуры, в которых используются АС. Несмотря на то, что общие принципы и подходы к защите различных отраслей несомненно существуют, необходимо учитывать специфику и потенциальные последствия кибератак для каждой из них.

Применительно к ядерной отрасли это могут быть: сложившаяся практика регулирования деятельности ядерных объектов; технические особенности их функционирования, включая необходимость непрерывного осуществления технологических процессов в течение долгого времени; исторически сложившаяся обособленность и закрытость ядерной отрасли; недостаточная осведомленность работников ядерных объектов о киберугрозах и их потенциальных последствиях для безопасности радиоактивных материалов и ядерных установок, а также ложное чувство защищенности ядерных объектов от киберугроз.

Чтобы оценить масштаб проблемы, надо иметь в виду, что АС используются для управления реакторами и установками по обогащению урана, сбора и анализа данных о параметрах ядерного объекта, управления транспортно‑техническими операциями с ядерными материалами и изделиями из них (например, перегрузкой топлива в активной зоне реактора) и т. П. Кроме того, на ядерных объектахавтоматизированными являются системы физической защиты ядерных объектов, учета и контроля ядерных материалов, различные системы документооборота и бухгалтерского учета.

Теоретически сбой в работе систем, обеспечивающих управление ядерной установкой, процессами обращения с ядерными материалами, а также элементами безопасности, призванными не допустить аварии, может привести к инциденту, последствия которого могут быть сравнимы с чернобыльской катастрофой.

Не менее пугающими выглядят сценарии отказа или ненадлежащего функционирования системы физической защиты ядерного объекта либо автоматизированной системы учета и контроля ядерных материалов вследствие кибератаки, равно как и хищение данных, с помощью которых злоумышленники могли бы найти способ обойти меры безопасности и похитить ядерные материалы с целью последующего создания ядерного взрывного устройства или *грязной* бомбы. Физическое воздействие на элементы ядерной установки, доступ к которым был получен при помощи кибератаки, может привести к радиационному загрязнению окружающей среды и облучению населения.

Помимо вышеупомянутых рисков, применение АС на ядерных объектах может создавать и другие, менее катастрофические риски, как‑то: убытки в результате нарушения бизнес‑процессов ядерного объекта, репутационные потери в результате хищения информации о функционировании объекта или разрушения имиджа объекта как надежно защищенного от злоумышленных воздействий.

В зависимости от того, какую цель преследуют злоумышленники (спровоцировать аварию, завладеть радиоактивными материалами или получить доступ к информации), кибератаки могут быть направлены на доступ, уничтожение, модифицирование, блокирование или копирование информации в соответствующих автоматизированных системах ядерного объекта.

## 4.4. Источники информации

В связи с существованием известных международных террористических организаций необходимо собирать информацию об угрозах как местного, так и национального и международного масштаба. К источникам такой информации относятся:

* разведывательные организации;
* криминологические исследования;
* профессиональные организации;
* публикуемая литература.

***Разведывательные организации*** могут предоставить подробную информацию о текущей деятельности групп, способных представлять угрозу атомным объектам. Важно получать и изучать такую текущую информацию постоянно.

***Криминологические исследования***. Изучение преступлений, совершенных в районе атомного объекта, в национальном и в международном масштабе в прошлом и в недавнее время, часто позволяет извлечь полезную информацию, характеризующую потенциальные виды угрозы.

***Профессиональные организации***. Неправительственные структуры обмена информацией позволяют получить сведения, полезные при оценке существующей угрозы. Ученые, исследователи и промышленные специалисты встречаются, чтобы обсудить проблемы и технологические достижения. Часто обсуждаются также вопросы и проблемы, связанные с обеспечением безопасности. Может быть создана структура информационного обмена в области обсуждения проблем, угрожающих безопасности предприятия на местном, национальном и международном уровне.

***Публикуемая литература***. Тщательное изучение доступной текущей литературы может привести к накоплению информации, относящейся к оценке существующей угрозы. Такую информацию можно получить из общедоступных источников, из библиотек и от исследовательских организаций. К общедоступным источникам текущей литературы относятся бюллетени национальных информационных агентств и периодические издания, передаваемые по радио и телевидению новости, труды, посвященные определенным вопросам. Важно сравнивать получаемую информацию со сведениями о других странах. В библиотеках и у исследовательских организаций имеются электронные базы данных, коллекции микрофильмов с выдержками из газет на определенные темы, справочные материалы по различным вопросам, значительно облегчающие поиск информации, имеющей отношение к потенциальной угрозе объекту.

## 4.5. Вероятные способы осуществления угроз

***Угрозы и вероятные способы их осуществления определяются на основе:***

а) рассмотрения разных видов угроз, применимых с точки зрения комиссии к данному объекту;

б) определения наиболее вероятных угроз для данного типа объекта;

в) оценки возможности реализации наиболее вероятных угроз (в качестве критерия принимается возможный ущерб от совершения акта незаконного вмешательства);

г) учета факторов, влияющих на вероятность осуществления угроз.

При определении угроз в отношении каждого критического элемента рассматриваются все возможные случаи прекращения нормального функционирования объекта, его повреждения или аварии вследствие акта незаконного вмешательства.

Методом экспертных оценок определяется базовая угроза, которая может быть осуществлена в отношении каждого критического элемента объекта.

При категорировании объекта комиссия определяет модель (тип) нарушителя для объекта и его критических элементов, которая используется для оценки эффективности принятых мер по защите объекта *(см. главу 2.4. Оценка эффективности системы физической защиты объекта).*

## 4.6. Модель нарушителя. Типы нарушителей

***Модель (тип) нарушителя*** представляет собой совокупность качественных и количественных характеристик нарушителя, его мотивации и преследуемых им целей и используется при определении требуемого уровня защищенности объекта и его критических элементов, выработке требований к системе физической защиты объекта и оценке ее эффективности (рисунок 20).

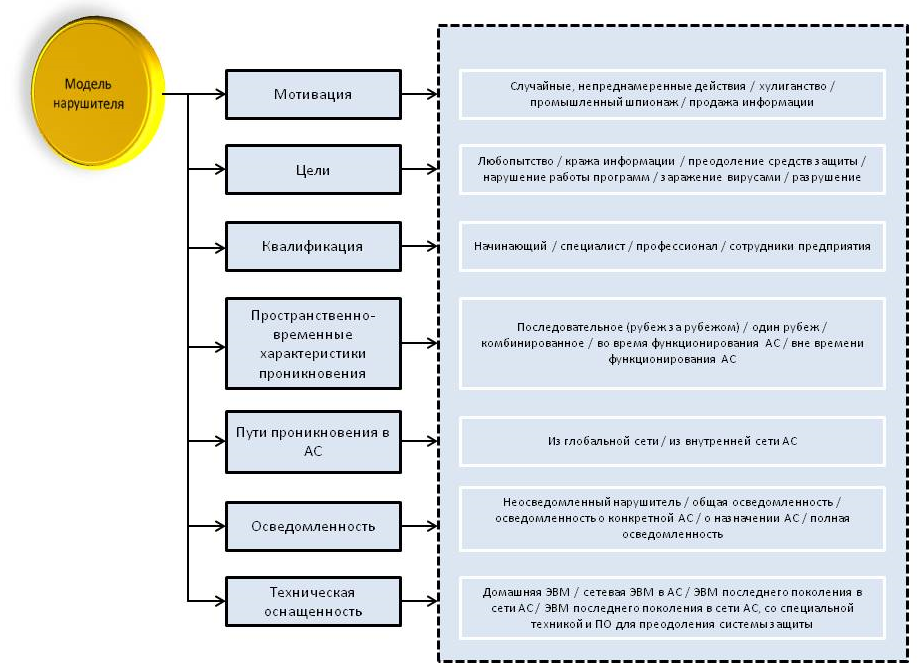


Рисунок 20. Типовая модель нарушителя.

***Типы нарушителей могут быть внешние и внутренние***.

Для проникновения в охраняемые зоны внешние нарушители могут использовать:

а) оружие для прорыва через контрольно-пропускные пункты (далее – КПП) и противодействия подразделениям охраны;

б) взрывные и зажигательные устройства и вещества для совершения террористического акта и преодоления инженерно-технических средств охраны (далее – ИТСО);

в) специальные средства, инструменты и снаряжение;

г) транспортные средства;

д) финансовые средства для подкупа внутренних нарушителей.

**Тактика действий нарушителей при проникновении на охраняемую территорию** может быть:

а) ***насильственной*** – с применением насилия по отношению к людям и с повреждением ИТСО;

б) ***обманной*** – создающей видимость санкционированности действий путем использования поддельных документов, ключей, идентификаторов личности и т.п.;

в) ***скрытной*** – когда нарушитель стремится остаться незамеченным;

г) ***комбинированной*** – различные сочетания вышеуказанных видов тактики.

В своих действиях нарушитель может применять любую тактику, повышающую шансы совершения акта незаконного вмешательства.

При определении модели нарушителя целесообразно использовать перечень потенциальных угроз в отношении объектов.

***Модели (типы) нарушителя подразделяются на:***

а) внешних нарушителей первого, второго и третьего типа;

б) внутренних нарушителей первого и второго типа.

### Внешние нарушители

***Внешний нарушитель первого типа*** – специально подготовленная террористическая группа (далее – ТГ) численностью от 3 до 20 человек, целью которой является совершение террористического акта.

Внешний нарушитель первого типа характеризуется:

а) осведомленностью о системе физической защиты объекта, его критических элементах, а также их технологических особенностях;

б) высокой вероятностью наличия холодного и огнестрельного оружия (в том числе автоматического), взрывных и зажигательных устройств (в том числе боевых);

в) высоким уровнем подготовки к преодолению ИТСО;

г) готовностью вступить в открытый вооруженный конфликт с подразделениями охраны объекта;

д) возможностью (в зависимости от численности) разделяться на отдельные, скоординированно действующие группы, решающие различные тактические задачи;

е) возможностью поражения опасными веществами (химическими, радиоактивными или биологическими агентами);

ж) возможным наличием в группе лиц, способных пожертвовать собой для достижения целей террористического акта.

***Наиболее вероятная тактика действий внешнего нарушителя первого типа*** – насильственная с вооруженным нападением и прорывом системы физической защиты (в том числе с применением транспортных средств), применение отвлекающего маневра, захват заложников (по необходимости).

***Внешний нарушитель второго типа –*** ***групповой нарушитель*** (далее – ГН) численностью 2 человека, не имеющий санкционированного доступа на территорию объекта, целью которого является совершение террористического акта.

Внешний нарушитель второго типа характеризуется:

а) осведомленностью о системе физической защиты объекта и его критических элементах, основанной на визуальном наблюдении;

б) высокой вероятностью наличия огнестрельного оружия;

в) возможным наличием взрывоопасных веществ;

г) возможностью использования легкого и специального инструмента;

д) высокой вероятностью использования автотранспорта;

е) подготовленностью к преодолению ИТСО.

***Наиболее вероятная тактика действий внешнего нарушителя второго типа*** – скрытное проникновение на территорию объекта и к его охраняемым критическим элементам.

Предполагается, что внешний нарушитель второго типа может вступить в сговор с работником охраны с целью сокрытия факта своего проникновения на территорию объекта.

***Внешний нарушитель третьего типа*** ***– специально подготовленный одиночный нарушитель*** (далее – ОН), не имеющий санкционированного доступа на территорию объекта, целью которого является совершение акта незаконного вмешательства.

Внешний нарушитель третьего типа характеризуется:

а) низким уровнем осведомленности о системе физической защиты объекта и его критических элементах, однако не исключается возможность того, что данный нарушитель действует по заранее спланированному сценарию;

б) высокой вероятностью наличия огнестрельного оружия;

в) вероятностью наличия взрывного устройства, предназначенного для совершения террористического акта;

г) возможностью поражения опасными веществами (химическими, радиоактивными или биологическими агентами);

д) низкой вероятностью использования автотранспорта;

е) высокой подготовленностью к преодолению ИТСО.

***Наиболее вероятная тактика действий внешнего нарушителя третьего типа*** – скрытное или обманное (с использованием поддельных документов) проникновение на территорию к объектам охраны.

### Внутренние нарушители

***Внутренний нарушитель первого типа –*** ГН из числа работников объекта, имеющий санкционированный доступ на территорию объекта и к его критическим элементам, целью которого является совершение акта незаконного вмешательства.

Внутренний нарушитель первого типа характеризуется:

а) высокой осведомленностью о технологических особенностях объекта и его критических элементах;

б) низкой вероятностью наличия огнестрельного оружия, взрывчатых веществ, ручного и строительного инструмента;

в) наличием легальных документов и возможностью беспрепятственного прохода.

***Внутренний нарушитель второго типа*** – ОН из числа сотрудников охраны или работников объекта, имеющий санкционированный доступ на территорию объекта. Целью такого нарушителя является сбор и передача важной информации террористам для совершения ими террористического акта.

Внутренний нарушитель второго типа характеризуется:

а) высокой осведомленностью о системе физической защиты или о технологических особенностях объекта;

б) высоким уровнем осведомленности о расположении постов охраны на территории объекта;

в) наличием штатного вооружения и специальных средств;

г) наличием легальных документов и возможностью беспрепятственного прохода на территорию объекта;

д) готовностью вступить в открытый вооруженный конфликт с подразделениями охраны.

***Наиболее вероятная тактика действий внутренних нарушителей*** – легальный проход на территорию объекта в рабочее время с использованием постоянного пропуска.

Внутренние нарушители могут принимать непосредственное участие в совершении террористического акта внешним нарушителем первого или второго типа, действуя по принуждению или по иным мотивам.

## 4.7. Формирование Перечня основных сценариев актов незаконного вмешательства

Результаты определения модели (типа) нарушителей заносятся в акт категорирования и паспорт безопасности объекта.

Комиссия проводит сравнительный анализ всех выявленных критических элементов объекта и с учетом их взаимовлияния выделяет те из них, совершение акта незаконного вмешательства на которых может привести к возникновению чрезвычайной ситуации с наибольшими социально-экономическими последствиями.

По результатам анализа уязвимости категорируемого объекта и с учетом потенциальных угроз в отношении объекта формируется перечень основных сценариев актов незаконного вмешательства в отношении критических элементов, совершение акта незаконного вмешательства на которых может привести к возникновению чрезвычайной ситуации с наибольшими социально-экономическими последствиями.

В качестве основных сценариев актов незаконного вмешательства могут рассматриваться:

а) захват (блокирование) объекта или одного из его элементов со взятием заложников;

б) взрыв объекта или его наиболее важного критического элемента с доставкой к периметру объекта с доступным подъездом или критическому элементу свыше 10 кг взрывчатых веществ;

в) взрыв критического элемента с доставкой к периметру объекта с доступным подъездом или критическому элементу до 10 кг взрывчатых веществ;

г) поражение объекта или его критического элемента опасными веществами;

д) хищение элементов объекта;

е) техническое воздействие (в том числе дистанционное) на системы электропитания, управления или защиты технологических процессов объекта;

ж) хищение секретной или конфиденциальной информации.

## 4.8. Формы взаимодействия со специализированными организациями

***К органам управления в системе физической защиты ЯОО относятся:***

Взаимодействие администрации ЯОО и его службы безопасности с подразделениями охраны осуществляется на следующих этапах создания и функционирования СФЗ:

* проектирование;
* строительство и монтаж;
* ввод в эксплуатацию;
* прием под охрану;
* повседневная деятельность;
* чрезвычайные ситуации и ликвидация их последствий;
* снятие с охраны.

К основным направлениям взаимодействия администрации ЯОО и его службы безопасности с подразделениями охраны при обеспечении физической защиты ЯОО относятся:

* оснащение ЯОО системами и средствами физической защиты;
* организация системы охраны, внесение частичных изменений в нее и реализация мероприятий по обеспечению надежности охраны;
* организация и осуществление пропускного и внутриобъектового режима;
* организация внутриобъектовой связи, предназначенной для обеспечения функционирования СФЗ, связи с взаимодействующими органами, организация радиоконтроля;
* взаимодействие СБ и подразделений охраны при действиях в штатных и чрезвычайных ситуациях (при авариях, пожарах, взрывах, нападениях на охраняемый объект и т.п.);
* проведение совместных контрольных проверок боевой службы караулов и контрольных проверок службы на постах с пропускными функциями;
* планирование и проведение совместных проверок работоспособности и состояния комплексов технических средств физической защиты (КИТСО);
* реконструкция и капитальный ремонт КТСФЗ (КИТСО);
* продление сроков эксплуатации и замена выработавших свой ресурс ИТСФЗ (ИТСО);
* техническое обслуживание ИТСФЗ (ИТСО);
* обучение и переподготовка технического персонала подразделений охраны;
* проведение совместных учений по оценке эффективности СФЗ;
* сбор и анализ статистической информации по помехоустойчивости и эксплуатационной надежности КТСФЗ (КИТСО);
* обеспечение безопасности персонала СФЗ ЯОО и личного состава подразделений охраны при выполнении задач физической защиты;
* управление и администрирование в автоматизированных СФЗ;
* обеспечение защиты информации;
* размещение, материально-техническое обеспечение подразделений, гарнизонов, застав, караулов, войсковых нарядов, комендатур и бюро пропусков.

***При проектировании и сооружении СФЗ, оснащении ЯОО инженерно-техническими средствами физической защиты осуществляются:***

* уточнение системы и способов охраны ЯОО;
* разработка структуры КТСФЗ (КИТСО);
* определение необходимой номенклатуры ТСФЗ (ТСО);
* определение необходимой номенклатуры инженерных средств физической защиты (ИСФЗ);
* определение сроков и порядка оборудования ЯОО комплексом ТСФЗ (ИТСО);
* разработка схемы организации связи ЯОО.

При организации системы охраны, внесении частичных изменений в нее и проведении мероприятий по обеспечению надежности охраны осуществляется:

* согласование состава, сроков и порядка работы межведомственной (внутренней) комиссии (МВК, ВК);
* определение в ходе работы МВК объектов, подлежащих охране на данном ЯОО, способов охраны, потребной численности охраны, количества и видов КПП, количества караулов (застав), их задач и объемов боевой службы, мероприятий по оборудованию ЯОО комплексами ТСФЗ (ИТСО) и созданию подразделениям охраны необходимых условий для выполнения задач физической защиты, порядка и сроков приема ЯОО под охрану (для новых объектов);
* разработка акта МВК об организации охраны, служебной документации караулов (застав) и контроль за реализацией предусмотренных актом мероприятий;
* определение в ходе работы ВК потребных изменений в системе охраны, сроков, на которые они производятся, порядка использования высвободившейся численности и мероприятий по дооборудованию ЯОО комплексами ТСФЗ (ИТСО);
* разработка акта ВК о частичных изменениях в системе охраны, уточнение служебной документации и контроль за реализацией предусмотренных актом мероприятий;
* проведение совместных обследований надежности охраны и реализация мероприятий по устранению выявленных недостатков;
* совершенствование КТСФЗ (КИТСО).

***При организации и осуществлении пропускного и внутриобъектового режима осуществляются:***

* выбор, согласование и утверждение инфраструктуры (центральное бюро пропусков, бюро пропусков на промышленных площадках, КПП городской зоны ЗАТО, КПП промышленных площадок, локальных зон);
* определение необходимой номенклатуры и количественных характеристик оборудования СФЗ;
* разработка структуры системы управления и контроля за доступом в охраняемые зоны;
* проектирование, сооружение, оснащение, испытания, аттестация, внедрение и эксплуатация системы управления и контроля за доступом в охраняемые зоны;
* разработка и согласование инструкции о пропускном режиме, инструкций лицам караула и табелей постам с пропускными функциями.

При организации внутриобъектовой связи, связи с взаимодействующими органами, радиоконтроля на основе федеральных, ведомственных и межведомственных нормативных документов, в том числе Положения о порядке использования систем радиосвязи на предприятиях Минатома России, осуществляются:

* выбор, согласование и утверждение основных и резервных каналов связи;
* определение необходимой номенклатуры и количественных характеристик оборудования связи;
* разработка внутриобъектовых нормативных документов о разработке и функционировании системы связи, а также их согласование с взаимодействующими органами;
* разработка схемы связи взаимодействия в штатном режиме и в чрезвычайных ситуациях;
* проектирование, сооружение, оснащение, испытания, внедрение и эксплуатация системы связи.

Взаимодействие администрации ЯОО, службы безопасности, подразделений охраны и других взаимодействующих органов в чрезвычайных ситуациях осуществляется согласно разработанных планов взаимодействия.

В планах взаимодействия на случай возникновения чрезвычайных ситуаций на ЯОО и при ликвидации их последствий должно предусматриваться привлечение внешней помощи в виде профессиональных аварийно-спасательных формирований и порядок взаимодействия с ними администрации ЯОО, службы безопасности и подразделений охраны.

***При планировании и проведении контрольных проверок боевой службы караулов и контрольных проверок службы на постах с пропускными функциями осуществляется:***

* изучение материалов предыдущих проверок;
* определение сроков проведения проверок, привлекаемых к ним лиц, объемов и порядка их проведения;
* составление планов проведения проверок;
* мероприятия по обеспечению скрытности и внезапности проведения проверок;
* анализ результатов проверок, подведение их итогов, определение и организация мероприятий по устранению вскрытых недостатков, повышению качества подготовки часовых постов с пропускными функциями и совершенствованию пропускного режима.

***Проверка работоспособности и технического состояния комплексов ТСФЗ (ИТСО) ЯОО осуществляется:***

1) представителями подразделений охраны самостоятельно (для комплексов, принятых ими в эксплуатацию), исходя из служебной необходимости, в сроки и объёмах, определяемых эксплуатационной документацией на ТСФЗ (ИТСО) и руководящими документами внутренних войск МВД России;

2) представителями службы безопасности самостоятельно (для комплексов, эксплуатируемых подразделением ИТСФЗ службы безопасности), исходя из служебной необходимости, в сроки и объёмах, определяемых эксплуатационной документацией на ТСФЗ (ИТСО);

3) совместными комиссиями с привлечением представителей внутренних войск МВД России и службы безопасности ЯОО – на основании распоряжений главного командования внутренних войск, командования округов и частей внутренних войск или администрации ЯОО:

а) ***при проведении:***

* годовых смотров ИТСФЗ (ИТСО) в сроки и объёмах, предусмотренных «Положением о смотре ИТСО на объектах, охраняемых ВВ МВД России»;
* внеплановых проверок ИТСФЗ (ИТСО) по инициативе командования частей внутренних войск МВД России;
* проверок надёжности охраны ЯОО по инициативе Минатома России, администрации ЯОО по отдельному графику или по мере необходимости;
* технического обслуживания ТСО специалистами ЯОО после его завершения в соответствии с планом-графиком проведения регламентных работ на ЯОО;

б) перед составлением годовых (перспективных) планов строительства, реконструкции и ремонта комплекса ТСФЗ (ИТСО) в полном объёме;

в) при продлении сроков эксплуатации выработавшей свой ресурс аппаратуры комплекса ТСФЗ (ИТСО) – ежегодно;

г) при вводе в эксплуатацию законченных строительством отдельных систем (элементов) или комплекса ТСФЗ (ИТСО) в целом, по мере окончания работ и завершения приёмо-сдаточных испытаний на основании «Программы и методики испытаний комплекса ТСФЗ (ИТСО) ЯОО»;

4) совместными комиссиями с привлечением представителей внутренних войск МВД России, службы безопасности ЯОО, государственных надзорных и контролирующих органов – на основании соответствующих распоряжений при проведении инспекционных проверок обеспечения физической защиты на ЯОО.

При комиссионных проверках работоспособности и технического состояния комплекса ТСФЗ (ИТСО) взаимодействие между подразделениями охраны и службой безопасности ЯОО организуется по срокам, объёмам и последовательности проверок, а также по совместно намечаемым мерам обеспечения пропускного режима и надёжности охраны ЯОО, на период проведения этих проверок.

При реконструкции и капитальном ремонте комплекса ТСФЗ (ИТСО) взаимодействие между подразделениями охраны и службой безопасности ЯОО организуется и осуществляется на этапах:

* разработки и согласования технического задания на проектирование комплекса ТСФЗ (ИТСО);
* предпроектного обследования, сбора и обобщения исходных данных для проектирования комплекса ТСФЗ (ИТСО);
* разработки и согласования рабочего проекта комплекса ТСФЗ (ИТСО);
* производства монтажных и пуско-наладочных работ;
* приемки рабочими комиссиями законченных строительством отдельных систем (элементов) или комплекса ТСФЗ (ИТСО) в целом;
* приёмо-сдаточных испытаний и комплексного опробования аппаратуры комплекса ТСФЗ (ИТСО);
* передачи аппаратуры комплекса ТСФЗ (ИТСО) в эксплуатацию подразделениям охраны.

При этом проводится:

* анализ состояния комплекса ТСФЗ (ИТСО), разработка и выдача проектной документации на реконструкцию и модернизацию ТСФЗ (ИТСО), определение материальных и финансовых затрат;
* приобретение оборудования, проведение строительно-монтажных и пуско-наладочных работ, сдача ТСФЗ (ИТСО) в эксплуатацию;
* разработка планов замены электронных средств обнаружения, выработавших эксплуатационный ресурс, создание резервного фонда аппаратуры.

Взаимодействие осуществляется в соответствии с проектной документацией и календарными планами на ремонт, реконструкцию и модернизацию СФЗ, разработанными на основе технических условий на ТСФЗ (ИТСО) и результатов анализа состояния комплекса ТСФЗ (ИТСО) и эффективности СФЗ, выполняемых службой безопасности совместно с эксплуатирующими ИТСО подразделениями.

При техническом обслуживании ИТСФЗ (ИТСО) взаимодействие осуществляется в соответствии с утвержденными планами обслуживания оборудования.

Взаимодействие по организации обучения и переподготовки технического персонала подразделений охраны осуществляется в соответствии с согласованными планами на предприятиях Минатома России или в учебных центрах внутренних войск МВД России по утверждённым методикам (программам обучения).

***При проведении совместных учений по проверке эффективности и взаимодействия осуществляются:***

* определение сроков учений, темы и основных целей учения;
* моделирование вероятного нарушителя, возможной тактики его действий для достижения цели;
* определение состава привлекаемых к учению сил физической защиты;
* выработка замысла учения и его утверждение;
* разработка плана проведения учения и других необходимых документов;
* подготовка руководителей и участников учения, обеспечение их необходимой материальной базы;
* проведение анализа в ходе учения;
* обеспечение безопасности участников учения и функционирования СФЗ;
* разбор результатов учения и его документирование;
* выявление уязвимых мест в СФЗ, выработка рекомендаций по устранению недостатков.

При сборе и анализе статистической информации по помехоустойчивости и эксплуатационной надёжности комплекса ТСФЗ (ИТСО) взаимодействие осуществляется в соответствии с утверждённой методикой на основании протокольных записей значимых событий в служебной, эксплуатационно-технической документации и базах данных.

При выполнении задач физической защиты для обеспечения безопасности персонала СФЗ ЯОО и личного состава подразделений охраны проводится:

* прогнозирование возможных для данного ЯОО аварийных ситуаций и их последствий;
* доведение результатов прогнозирования до персонала службы безопасности и подразделений охраны;
* планирование действий персонала службы безопасности и подразделений охраны в условиях аварийных ситуаций;
* изучение влияния вредных факторов производственной деятельности ЯОО на персонал СФЗ и принятие мер по их снижению;
* обеспечение персонала службы безопасности и подразделений охраны средствами защиты, радиационной разведки, дозиметрического контроля, специальной одеждой (по необходимости) и противорадиационными препаратами;
* согласование вопросов использования защитных сооружений ЯОО.

***При управлении и администрировании в автоматизированных СФЗ решаются вопросы:***

* взаимодействия центрального пункта управления с пунктами управления различного уровня и функционального назначения;
* распределения задач по управлению СФЗ с пунктов управления различного уровня и функционального назначения;
* распределения полномочий администраторов в единой интегрированной СФЗ.

При этом управление может осуществляться как с центрального пункта управления (ЦПУ) системой физической защиты ЯОО в целом, так и с локальных пунктов управления (ЛПУ) системами физической защиты отдельных внутренних ЯОО (промышленных площадок, отдельных зданий и сооружений), также с локальных пунктов, предназначенных для управления отдельными функциональными подсистемами СФЗ.

3ащита информации осуществляется в соответствии с Концепцией информационной безопасности СФЗ ЯОО, Общими требованиями по защите информации в СФЗ ЯОО и временным руководящим документом «Система физической защиты ЯОО. Автоматизированные системы управления и обеспечения физической защиты. Защита информации от несанкционированного доступа. Классификация автоматизированных систем и требования по безопасности информации».

Взаимодействие осуществляется при согласовании нормативных документов объектового уровня по защите информации.

При размещении, материально-техническом обеспечении подразделений, гарнизонов, застав, караулов, войсковых нарядов, комендатур и бюро пропусков решаются вопросы, изложенные в акте МВК об организации охраны объекта, а также другие вопросы обеспечения их деятельности и благоустройства.

Порядок взаимодействия излагается в планах взаимодействия администрации, службы безопасности, подразделений охраны и персонала ЯОО в штатном режиме и в чрезвычайных ситуациях, в планах взаимодействия администрации, службы безопасности и подразделений охраны ЯОО с органами внутренних дел и ФСБ России в штатном режиме и в чрезвычайных ситуациях, профессиональными аварийно-спасательными формированиями МЧС России в чрезвычайных ситуациях.

***В планах взаимодействия должны определяться:***

* разрабатываемые сторонами документы по физической защите ЯОО, в которых отражаются вопросы взаимодействия;
* права, обязанности сторон и их конкретные действия в штатных и чрезвычайных ситуациях;
* разделение сфер ответственности сторон в области физической защиты.

***При организации взаимодействия администрация ЯОО совместно с командованием подразделений охраны обязаны согласовать:***

* совместные мероприятия по обеспечению надежности охраны объектов;
* порядок осуществления пропускного и внутриобъектового режима;
* объем и сроки оборудования объектов, контролируемых зон ИТСФЗ (ИТСО);
* мероприятия по размещению и материально-техническому обеспечению подразделений, гарнизонов, караулов, войсковых нарядов, комендатур объектов;
* порядок выделения транспортных средств для обеспечения выполнения задач подразделениями, караулами, войсковыми нарядами, в том числе при осложнении обстановки;
* порядок привлечения сил и средств администрации объектов при чрезвычайных ситуациях;
* меры безопасности личного состава при выполнении служебно-боевых задач и на случай производственной аварии с выбросом радиоактивных и сильнодействующих ядовитых веществ.

***Разделение ответственности службы безопасности и подразделений охраны в управлении СФЗ***

Вопросы разделения ответственности по управлению СФЗ ЯОО между администрацией ЯОО и ее СБ, с одной стороны, и воинскими частями (подразделениями), осуществляющими охрану ЯОО, должны решаться на всех этапах проектирования, сооружения, эксплуатации, реконструкции и вывода из эксплуатации СФЗ.

Кроме того, должны быть решены вопросы разделения ответственности по управлению СФЗ ЯОО между различными иерархическими уровнями управления.

***При определении мер ответственности сторон должны учитываться:***

* категория ЯОО, особенности его размещения и условия функционирования;
* наличие и характер охраняемых зон (защищенной, внутренней, особо важной, локальной высоко-опасной), зон ограниченного доступа;
* пропускной режим;
* система и способ охраны указанных зон;
* степень их оснащенности системами и средствами физической защиты;
* наличие на объекте автоматизированных СФЗ, степень и перспективы их интеграции;
* состояние и уровень проработки нормативной документации в области физической защиты;
* количественный и качественный состав подразделений СБ и подразделений охраны, их уровень подготовки и технической оснащенности подразделений.

Для всех категорий ЯОО подразделения внутренних войск в соответствии с актами межведомственных комиссий об организации охраны ЯОО могут охранять периметры территорий, КПП и режимные помещения.

Подразделения внутренних войск, как правило, охраняют защищенные зоны и периметры внутренних зон ЯОО и обеспечивают работоспособность принятых в установленном порядке в эксплуатацию и обслуживаемых ими средств и систем физической защиты, а также управление СФЗ указанных зон с соответствующих пунктов управления.

В зависимости от категории ЯОО, условий его функционирования и особенностей размещения охраняемых зон на основании разрешительной системы допуска исполнителей и командированных лиц к секретным работам, сведениям, документам, к ядерным материалам и установкам администрацией ЯОО могут быть наложены ограничения не только на доступ персонала подразделений внутренних войск в те или иные зоны и помещения и получение из них операторами соответствующих пунктов управления и начальником караула визуальной информации с помощью средств телевизионного наблюдения, но и на работу с системами управления и контроля доступом персонала ЯОО в эти зоны и помещения.

В этом случае функции охраны внутри этих охраняемых зон выполняют подразделения СБ ЯОО (ведомственной охраны).

Обеспечение функционирования СФЗ на периметрах особо важных зон в зависимости от конкретных условий расположения и особенностей функционирования ЯОО в соответствии с актом межведомственной комиссии об организации охраны может осуществляться подразделениями охраны.

При этом подразделения охраны несут ответственность за работоспособность и обслуживание средств и систем физической защиты, принятых в эксплуатацию, на периметрах особо важных зон, за исключением систем управления и контроля доступа в эти зоны, а также за управление СФЗ указанных зон с пунктов управления с учетом указанного ограничения.

В последнем случае системы управления и контроля доступа в особо важные зоны эксплуатируются службой безопасности ЯОО (ведомственной охраной).

Во всех случаях обеспечение функционирования СФЗ локальных высоко-опасных зон, ответственность за работоспособность и обслуживание средств и систем физической защиты этих зон, а также за управление СФЗ указанных зон с соответствующих пунктов управления и с ЦПУ несет служба безопасности ЯОО (ведомственная охрана).

Порядок допуска личного состава подразделений охраны, а также персонала других взаимодействующих органов в особо важные и локальные высоко-опасные зоны, а также в соответствующие зоны ограниченного доступа при чрезвычайных ситуациях определяется инструкцией о пропускном режиме, а действия подразделений внутренних войск и службы безопасности (ведомственной охраны) в этих ситуациях определяются соответствующими планами взаимодействия.

## 4.9. Порядок определения угроз и модели нарушителя

### Определение угроз

Порядок определения угроз и модели нарушителя регламентирован Приказом Федеральной службы по экологическому, технологическому и атомному надзору от 14 декабря 2016 г. N 535 «Об утверждении руководства по безопасности при использовании атомной энергии «Рекомендации по проведению анализа уязвимости радиационного объекта».

Согласно данному документу, угрозы рекомендуется определять на основании перечня основных угроз ядерно и радиационно опасным объектам и типовых моделей нарушителей.

Под угрозой для радиоактивных веществ, радиационных источников и пунктов хранения понимается совокупность условий и факторов, создающих возможность совершения хищения радиоактивных веществ или радиационных источников либо диверсии.

При определении угроз для радиоактивных веществ, радиационных источников и пунктов хранения рассматриваются угрозы, связанные с преднамеренными целенаправленными действиями нарушителей, определенных в модели нарушителей.

Угрозы рекомендуется определять по отношению к каждому конкретному радиационному объекту и документировать в виде перечня угроз для конкретного радиационного объекта.

При определении каждой угрозы рекомендуется установить следующий набор характеристик исходя из собранной информации о радиационных объектах и находящихся на них радиоактивных веществах, радиационных источниках, пунктах хранения:

1) результат в случае реализации угрозы нарушителями (хищение радиоактивных веществ, радиационных источников или диверсия);

2) вероятный способ осуществления хищения или диверсии (например, взлом, подрыв, скрытое изъятие, повреждение элементов, систем, оборудования, устройств радиационных источников и пунктов хранения);

3) местоположение внутренних и внешних нарушителей, необходимое для реализации хищения или диверсии;

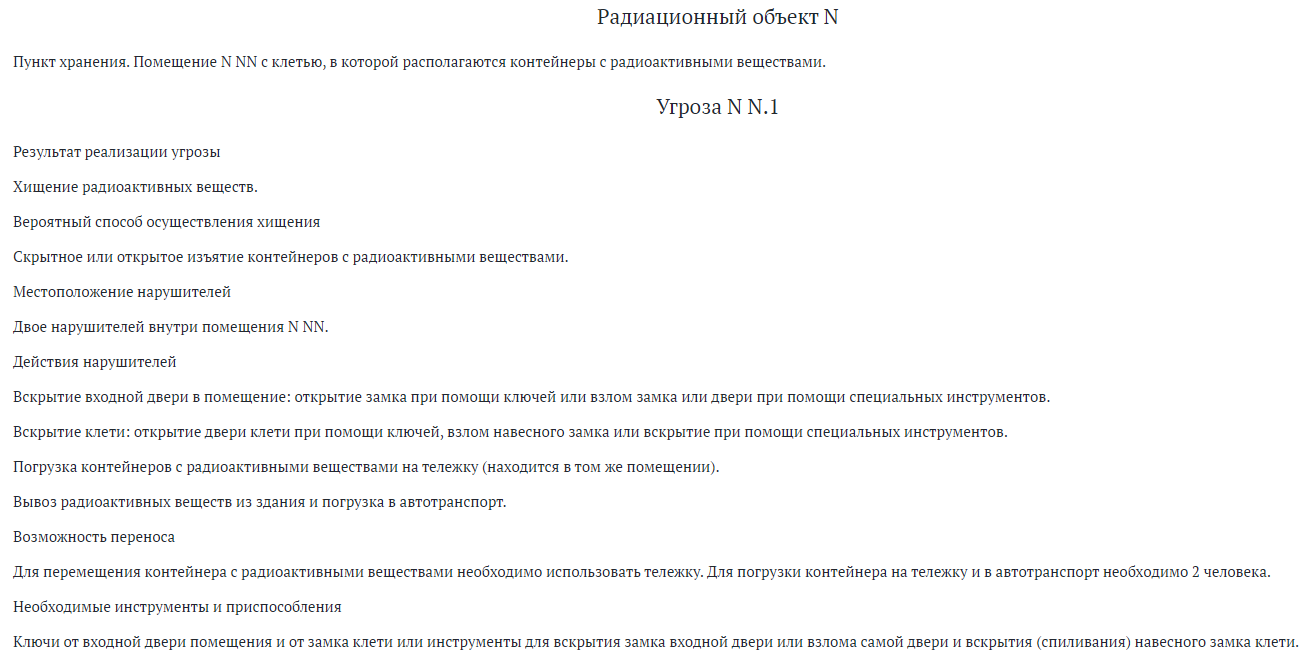
4) действия нарушителей, необходимые для совершения хищения или диверсии (рекомендуется учитывать результаты выявления уязвимых мест);

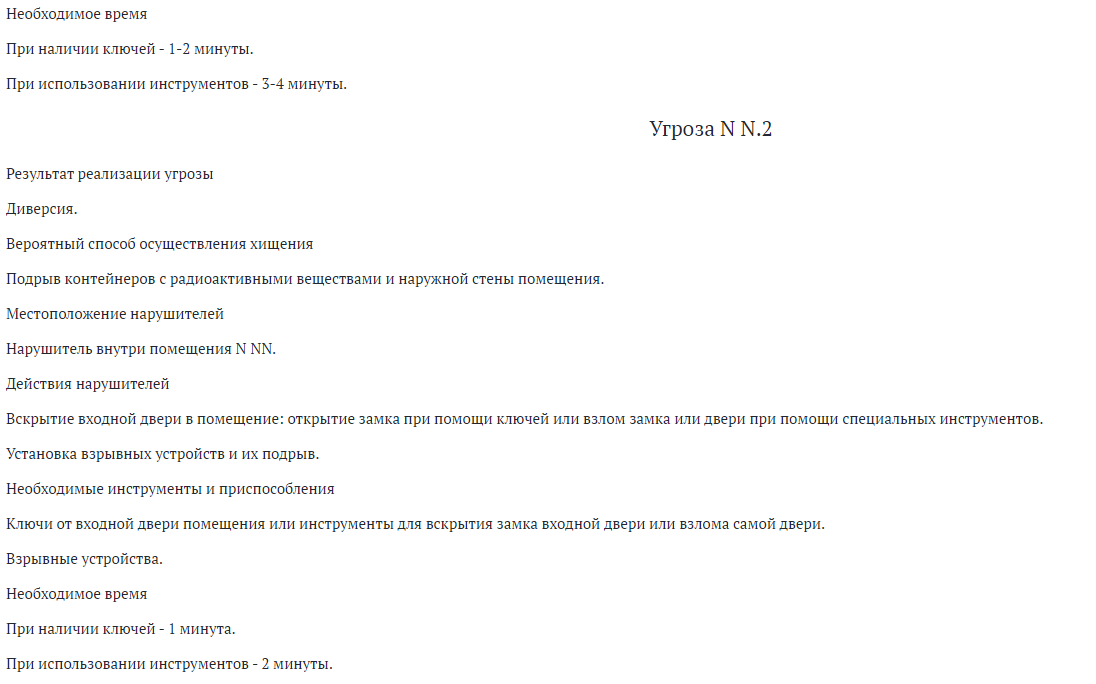
5) для угроз хищения – возможность переноса радиоактивных веществ, радиационного источника и/или закрытого радионуклидного источника одним человеком, группой лиц, необходимость использования тележки или транспортного средства для перевозки, подъемного механизма для погрузки радиоактивных веществ или радиационного источника;

6) перечисление необходимых для реализации хищения или диверсии инструментов и приспособлений;

7) указание необходимого нарушителям времени для совершения диверсии или хищения.

Пример описания угроз приведен ниже.





Указанный выше состав характеристик рекомендуется не рассматривать как исчерпывающий при определении угроз. По решению рабочей группы могут определяться дополнительные характеристики и особенности угроз.

Результаты определения угроз рекомендуется использовать при подготовке модели нарушителей.

### Определение модели нарушителей

Модель нарушителей для конкретной организации определяется на основании перечня основных угроз ядерно и радиационно опасным объектам и типовых моделей нарушителей.

При установлении модели нарушителей рекомендуется определять сведения и характеристики, необходимые и достаточные для реализации хищения или диверсии с учетом возможностей действий нарушителей.

Для формирования модели нарушителей рекомендуется собрать информацию обо всех случаях совершения преступлений на близлежащих объектах, аналогичных тем, которые могут произойти в организации.

Рекомендуется документировать используемые источники информации, а также принятые допущения при их анализе.

Рекомендуется в модель нарушителей включать несколько типов потенциальных нарушителей. Для каждого типа потенциальных нарушителей рекомендуется:

1) по признаку права доступа в защищенную зону и на радиационные объекты выделить:

* внутренних нарушителей, имеющих право доступа в защищенную зону и на радиационные объекты, к радиоактивным веществам и радиационным источникам;
* внешних нарушителей, не имеющих указанных прав доступа;
* внешних нарушителей, действующих в сговоре и с помощью внутренних нарушителей (совместно);

2) для внутренних нарушителей выделять группы нарушителей, имеющих санкционированный доступ в определенные защищенные зоны и на радиационные объекты, для каждой группы внутренних нарушителей рекомендуется указывать порядок доступа в рабочее и нерабочее время, выходные и праздничные дни, в штатных и чрезвычайных ситуациях;

3) по признаку цели совершения хищения или диверсии выделять категории нарушителей: террористы (диверсанты), преступники, экстремисты, пособники другим категориям нарушителей, нарушители внутриобъектового режима;

4) определить следующие характеристики нарушителей:

* виды мотивации нарушителей: политические, идеологические, экономические (получение материальной выгоды), экологические, личные;
* максимальное количество в группах внешних и внутренних нарушителей;
* тип вооружения, которым могут пользоваться нарушители соответствующих типов, групп и категорий;
* инструменты и приспособления, которые могут использовать нарушители при преодолении физических барьеров и вскрытии защитных конструкций;
* транспортные средства, которые могут использовать нарушители при движении к объекту и на его территории;
* степень осведомленности нарушителей (о расположении зданий, сооружений, дорог (дорожек) и физических барьеров; о характере радиоактивных веществ, радиационных источников и пунктов хранения и их размещении в зонах, зданиях, помещениях; о системе физической защиты, размещении сил охраны, порядке доступа на объект, в его здания, помещения и сооружения);
* степень подготовленности нарушителей к совершению хищения или диверсии: уровень обычной подготовки, основанный на изучении открытой информации и на самоподготовке, уровень общей военной подготовки воинских подразделений общего назначения или частных охранных предприятий, уровень подготовки войск специального назначения или специальной подготовки в террористических организациях;

5) установить тактику действий нарушителей, которая включает следующие характеристики:

* формы совершения хищения и диверсии (например, открытое нападение на объект с прорывом через физические барьеры физической защиты, подавлением или уничтожением оказывающих сопротивление сил охраны и персонала объекта; скрытое совершение хищения или диверсии с преодолением контрольно-пропускных пунктов обманным путем, со скрытым преодолением физических барьеров физической защиты ухищренными способами, с обходом средств обнаружения, блокированием выдачи сигналов тревоги и телевизионных изображений, с маскировкой от распознавания телевизионными средствами наблюдения, со скрытым уходом с объекта после совершения хищения или диверсии; комбинированная форма, включающая скрытое проникновение на радиационные объекты и к местам размещения сил охраны (зданиям караулов) с последующим открытым нападением, подавлением или уничтожением сил охраны, открытый прорыв за территорию объекта после совершение хищения или диверсии);
* возможные способы преодоления физических барьеров физической защиты;
* возможные способы прохода, проезда через контрольно-пропускные пункты;
* возможные способы проноса (провоза) оружия, взрывчатых веществ и иных специальных средств и приспособлений;
* возможность захвата средств и приспособлений, а также транспортных средств, расположенных на территории организации;
* возможность проникновения нарушителей через прилегающую акваторию на плавсредстве или с использованием аквалангов;
* тактика ведения боя.

Пример описания модели нарушителей приведен ниже.

### Пример описания модели нарушителей

**1. Тип потенциальных нарушителей N 1:  
одиночный внутренний нарушитель**

1.1. Имеет право доступа в защищенную зону и на радиационный объект, к радиоактивным веществам и радиационным источникам в рабочее время в штатных ситуациях.

1.2. Любой из работников, работающих в организации, за исключением персонала физической защиты, который проходит специальную проверку службой безопасности, рассматривается как потенциальный внутренний нарушитель. Для внутреннего нарушителя предполагается наличие права доступа на любой радиационный объект (но не на все сразу).

1.3. Категория нарушителя: экстремист (террорист).

1.4. Мотивация: идеологическая (религиозная).

1.5. Тип вооружения: индивидуальное стрелковое оружие (пистолет-пулемет).

1.6. Используемые инструменты и приспособления: отмычки, ручные инструменты.

1.7. Транспортные средства: легковой автомобиль.

1.8. Степень осведомленности:

- хорошая осведомленность о режиме работы организации, расположении зданий и сооружений в организации, радиационных объектов и радиоактивных веществ, радиационных источников и пунктов хранения на них, порядке доступа;

- общие представления о системе физической защиты, размещении сил охраны.

1.9. Степень подготовленности нарушителя: отсутствует профессиональная военная подготовка.

1.10. Тактика действий нарушителя.

Формы совершения хищения и диверсии: проход на радиационный объект с использованием права доступа и последующим скрытым или открытым (с использованием оружия) покиданием территории организации.

Возможными способами прохода через контрольно-пропускные пункты являются:

- открытый проход через контрольно-пропускной пункт без взрывчатых веществ и оружия;

- открытый проход через контрольно-пропускной пункт со скрытным проносом взрывчатых веществ и оружия.

Возможны попытки скрытого преодоления физических барьеров путем обхода технических средств охранной сигнализации при проникновении на объект и открытого преодоления физических барьеров, минуя контрольно-пропускные пункты при покидании организации за счет хорошей осведомленности об объекте.

Возможна попытка скрытного проноса (протаскивания) взрывчатых веществ и оружия через физические барьеры.

Возможно использование нарушителем средств и приспособлений, а также транспортных средств, расположенных на территории организации.

Нарушитель может применить стрелковое оружие.

**2. Тип потенциальных нарушителей N 2:  
внешний нарушитель в сговоре с внутренним нарушителем**

2.1. Внутренний нарушитель имеет право доступа в защищенную зону и на радиационный объект, к радиоактивным веществам и радиационным источникам в рабочее время в штатных ситуациях.

Внешний нарушитель прав доступа не имеет, действует в сговоре с внутренним нарушителем.

2.2. Любой из работников, работающих в организации, за исключением персонала физической защиты, который проходит специальную проверку службой безопасности, рассматривается как потенциальный внутренний нарушитель. Для внутреннего нарушителя предполагается наличие права доступа на любой радиационный объект (но не на все сразу).

2.3. Категория нарушителей: экстремист (террорист), пособник экстремиста (террориста).

2.4. Мотивация:

- у внешнего нарушителя – идеологическая (религиозная);

- у внутреннего – получение материальной выгоды, личные мотивы, принуждение.

2.5. Количество нарушителей: 1 внешний и 1 внутренний.

2.6. Тип вооружения: у внешнего нарушителя – индивидуальное стрелковое оружие (пистолет-пулемет, штурмовая винтовка), взрывчатые боеприпасы; у внутреннего нарушителя – индивидуальное стрелковое оружие (пистолет-пулемет).

2.7. Используемые инструменты и приспособления: сотовые телефоны, отмычки, ручные инструменты, лестницы.

2.8. Транспортные средства: легковой или грузовой автомобиль.

2.9. Степень осведомленности:

- хорошая осведомленность о режиме работы организации, расположении зданий и сооружений в организации, радиационных объектов и радиоактивных веществ, радиационных источников и пунктов хранения на них, порядке доступа;

- хорошая осведомленность о принципах работы технических средств физической защиты, общие представления о системе физической защиты объекта, размещении сил охраны.

2.10. Степень подготовленности нарушителя:

- у внешнего нарушителя – уровень подготовки войск специального назначения или специальной подготовки террористических организаций;

- у внутреннего нарушителя – отсутствует профессиональная военная подготовка.

2.11. Тактика действий нарушителей.

Формы совершения хищения и диверсии: скрытое проникновение на радиационный объект внутреннего нарушителя с последующим открытым нападением внешнего нарушителя, подавлением или уничтожением сил охраны, далее – открытый прорыв за территорию защищенной зоны.

Возможными способами прохода через контрольно-пропускные пункты для внутреннего нарушителя являются:

- открытый проход через контрольно-пропускной пункт без взрывчатых веществ и оружия;

- открытый проход через контрольно-пропускной пункт со скрытным проносом взрывчатых веществ и оружия.

Возможным способом прохода внешнего нарушителя через контрольно-пропускные пункты является силовой прорыв с использование оружия и взрывчатых веществ.

Возможны попытки скрытого преодоления физических барьеров путем обхода технических средств охранной сигнализации при проникновении на объект и открытого преодоления физических барьеров, минуя контрольно-пропускные пункты при покидании организации за счет хорошей осведомленности об объекте.

Возможна попытка скрытого проноса (протаскивания) внутренним нарушителем взрывчатых веществ и оружия через физические барьеры.

Возможно использование нарушителями средств и приспособлений, а также транспортных средств, расположенных на территории организации.

Возможен захват заложников, а также выполнение роли заложника внутренним нарушителем.

Внешний нарушитель будет вести открытое нападение с применением оружия. Внутренний нарушитель может применить стрелковое оружие по ситуации.

**3. Тип потенциальных нарушителей N 3:  
группа внешних нарушителей**

3.1. Внешние нарушители прав доступа не имеют.

3.2. Категория нарушителей: экстремист (террорист).

3.3. Мотивация: идеологическая (религиозная).

3.4. Количество нарушителей: группа из 2 человек с возможным разделением для проникновения на объект из разных мест.

Тип вооружения: индивидуальное стрелковое оружие (пистолет-пулемет, штурмовая винтовка), взрывчатые боеприпасы.

3.5. Используемые инструменты и приспособления: радиостанции, сотовые телефоны, отмычки, ручные инструменты, лестницы.

3.6. Транспортные средства: легковой или грузовой автомобиль.

3.7. Степень осведомленности: общее расположение зданий и сооружений, хорошая осведомленность о принципах работы технических средств физической защиты.

3.8. Степень подготовленности нарушителя: уровень подготовки войск специального назначения или специальной подготовки террористических организаций.

3.9. Тактика действий нарушителей.

Формы совершения хищения и диверсии: открытое нападение на объект (прорыв через физические барьеры физической защиты, подавление или уничтожение оказывающих сопротивление сил охраны и персонала объекта).

Внешний нарушитель осуществляет силовой прорыв через контрольно-пропускные пункты с использованием оружия и взрывчатых веществ.

Возможны проникновение и покидание объекта путем открытого преодоления физических барьеров.

Возможно использование нарушителем средств и приспособлений, а также транспортных средств, расположенных на территории организации.

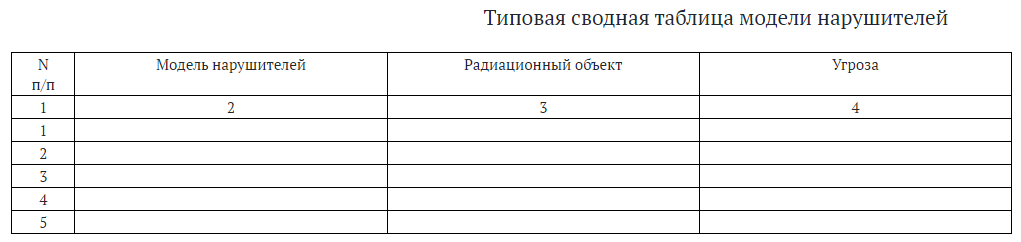
Возможен захват заложников.

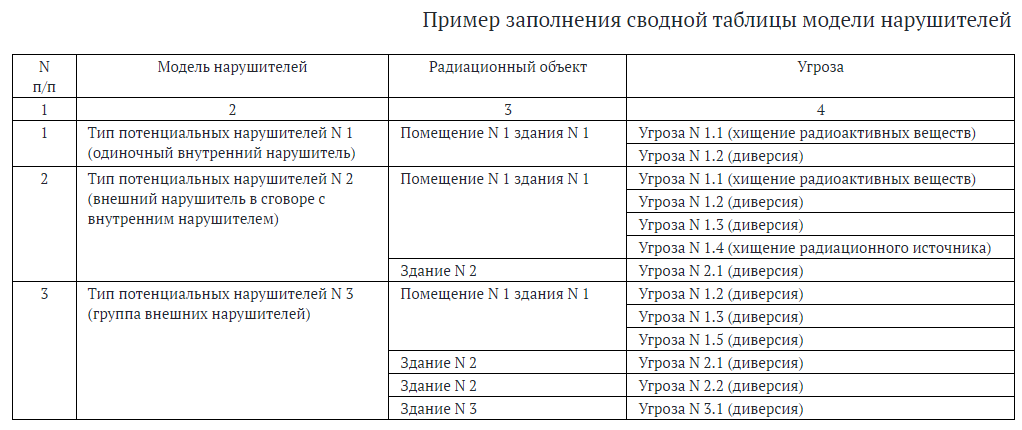
Нарушители будут вести открытое нападение с применением оружия. Проникновение на объект возможно с разных направлений.

Указанный выше состав характеристик рекомендуется не рассматривать как исчерпывающий при определении модели нарушителей. По решению рабочей группы могут определяться дополнительные характеристики и особенности типов потенциальных нарушителей.

По результатам определения модели нарушителей рекомендуется готовить документ, устанавливающий модель нарушителей, который утверждается руководителем организации и направляется для согласования с территориальным органом безопасности.

В документе, устанавливающем модель нарушителей, рекомендуется привести описание угроз, описание каждого типа потенциальных нарушителей, а также привести сводную таблицу, в которой для каждого типа потенциальных нарушителей из модели нарушителей указываются радиационный объект, на котором нарушитель способен совершить хищение или диверсию, и реализуемые им угрозы. Типовая сводная таблица модели нарушителей и пример ее заполнения приведены ниже.





Документ, устанавливающий модель нарушителей, рекомендуется пересматривать не реже, чем раз в пять лет.

## 4.10. Реализация угроз

Разработчикам систем физической защиты ядерного объекта важно правильно оценивать *проектные угрозы*, то есть понимать, кто и каким образом может попытаться совершить противоправные действия в отношении предметов защиты. Возможные злоумышленники разнятся от фанатиков‑одиночек, смутно представляющих себе принципы функционирования ядерного объекта, до хорошо вооруженных преступных групп, обладающих знаниями и технологиями, необходимыми для управления ядерной установкой, имеющих возможность удаленного доступа к управлению системами объекта и действующих в сговоре с персоналом ядерного объекта.

Чтобы выявить реальные угрозы и сценарии их осуществления для каждого конкретного объекта необходимо провести тщательный анализ криминогенной и социальной обстановки, угроз безопасности, признанных на уровне государства и отрасли, степени риска для имеющихся радиоактивных материалов, потенциальных последствий аварий и возможных путей воздействия на элементы ядерной установки с целью вызвать ядерный инцидент.

### Диверсия на ядерном объекте

В настоящее время мишенями для ядерного терроризма могут стать различные объекты ядерной инфраструктуры: АЭС, исследовательские реакторы, заводы по производству уранового концентрата, обогатительные предприятия, атомные электростанции, хранилища и установки по переработке отработанного топлива. Как показывает информация МАГАТЭ, далеко не все они защищены в должной мере. Еще одним сценарием радиологического терроризма является захват транспортного средства, перевозящего отработанное ядерное топливо или отходы с высоким уровнем радиации.

Аварии на ЧАЭС и Фукусиме показали, насколько тяжелыми могут быть последствия ядерной аварии. Между тем, то, что произошло по случайному стечению обстоятельств, вполне может быть повторено преднамеренно.

Диверсия на ядерном объекте не требует столь глубоких научных и технических познаний, как изготовление ядерной бомбы. Достаточно проникновения на объект группы боевиков со стрелковым оружием и взрывчаткой.

При диверсии на АЭС приоритетной целью для террористов могут стать охлаждающие системы. Если их вывести из строя, вероятность радиоактивного выброса резко возрастает. Террористы могут попытаться разрушить обслуживающие системы реактора, а также системы подачи воды, управления и защиты для того, чтобы вызвать тепловой взрыв в реакторе с его последующим разрушением, а также разрушение здания, в котором он находится. Даже если нападающие добьются не взрыва реактора, а всего лишь его остановки, все равно это будет иметь масштабные экономические и социально-политические последствия. Возможен также спуск террористами воды, используемой для охлаждения реактора (именно это случилось на «Фукусиме», правда, не вследствие злонамеренных действий).

В США и России власти осознали возможные последствия терактов на ядерных объектах, и в последние годы повышенное внимание уделяется усилению их безопасности. Так, в ходе учений федеральных спецслужб США были вскрыты существенные просчеты в охране Лос-Аламосской ядерной лаборатории, позволившие агентам, исполнявшим роль террористов, преодолеть охрану и прорваться на территорию объекта.

В России специальным постановлением правительства был утвержден перечень радиационно и ядерно опасных объектов. Помимо военных объектов, в него вошли несколько десятков важнейших объектов бывшего Минатома, энергоблоков АЭС, реакторы по производству оружейных материалов, радиохимические предприятия по переработке отходов ядерного топлива и его хранилища, заводы по сборке и утилизации ядерных боеприпасов.

Необходимо отметить, что после Чернобыля безопасность АЭС была значительно повышена. Даже если предположить, что террористы захватили пульт управления АЭС, и пытаются разогнать реактор с целью вызвать взрыв, у них, скорее всего, ничего не получится, так как реактор будет заглушен автоматикой защиты. В случае опасности захвата реактора он также будет немедленно остановлен.

С другой стороны, крепость цепи будет определяться крепостью самого слабого его звена. Очевидно, что террористы не так глупы, чтобы атаковать высокозащищенный ядерный объект. Скорее всего, в качестве цели ими будет выбран объект, где меры безопасности недостаточны.

### Киберинциденты

Для оценки возможных последствий кибератак с точки зрения СФЗ ЯО рассмотрим несколько сценариев, основанных на данных об имевших место киберинцидентах.

В качестве первого примера возьмем кибератаку в отношении обогатительной установки в иранском городе Натанз. Как известно, для нападения использовался вирус Stuxnet, перепрограммировавший промышленные контроллеры таким образом, что они отдавали установке *несовместимые с жизнью* управляющие команды, игнорируя данные датчиков, которые в нормальных условиях должны были привести к выдаче команды на перевод установки в безопасный режим. Пострадавший объект считался защищенным от вирусов в связи с отсутствием физического подключения к интернету, однако вредоносная программа была занесена в его систему управления с внешнего носителя.

Теперь представим, что системы безопасности АЭС, призванные локализовать и/или предотвратить аварию, построены на основе программируемых контроллеров, а каналы защиты с жесткой логикой не предусмотрены или выведены из строя. Атака вируса, действующего подобно Stuxnet, может перепрограммировать контроллеры систем безопасности таким образом, что при достижении определенных параметров (например, давления, температуры или реактивности), они не сработают, но сообщат оператору о срабатывании. Другими словами, произойдет отказ систем безопасности, который не будет вовремя обнаружен персоналом. При бездействующих системах безопасности авария, спровоцированная действиями злоумышленников или случайным стечением обстоятельств, может принять катастрофические масштабы.

Другим примером может стать получение удаленного доступа к автоматизированной системе с помощью программного обеспечения для создания VPN, применяемого поставщиком оборудования системы физической защиты, IP‑адресов оборудования системы физической защиты, имени пользователя и пароля, используемых по умолчанию. Эта информация может быть получена различными способами, включая кибератаки на поставщиков оборудования, подкуп, обман или шантаж персонала. Путем удаленного управления элементами системы физической защиты злоумышленники могут обеспечить себе беспрепятственный проход в охраняемые зоны объекта и выход из них, одновременно заблокировав проход для персонала. Изображение с камер видеонаблюдения может быть *зациклено* таким образом, чтобы демонстрировать оператору отснятую ранее картинку пустого помещения в то время, как в нем находятся злоумышленники. В результате преступники смогут совершить задуманное, например, похитить ядерные материалы или осуществить диверсию и беспрепятственно покинуть объект.

Весьма эффективный способ скомпрометировать корпоративную сеть — рассылка во внутренней сети предприятия фишинговых сообщений, через которые может быть загружен вирус, способный выкрасть чертежи и схемы ядерной установки. Полученная информация может затем быть использована преступниками для выявления наиболее эффективных способов диверсии или хищения радиоактивных материалов.

При этом важно понимать, что вышеописанные сценарии могут иметь комбинированный характер. Злоумышленники могут совершать кибератаки не только с непосредственно диверсионными целями, но и для подготовки диверсий или усиления их негативных последствий.

Кибератаки могут осуществляться удаленно, либо с территории ядерного объекта. Во втором случае злоумышленнику необходимо получить физический доступ к элементам ядерной установки или обеспечить подключение носителя с вредоносным программным обеспечением к элементам установки. Проще всего сделать это при содействии персонала ядерного объекта или подрядных организаций. Сценарии осуществления угроз могут включать кибератаки следующих типов:

* Кибератаки на автоматизированные системы управления технологическими процессами (АСУ ТП) ядерной установки. Они могут быть направлены на изменение или блокирование управляющих команд, блокирование доступа операторов к информации о состоянии ядерного объекта или искажение такой информации, а также на перепрограммирование промышленных контроллеров. Целью кибератаки может быть инициирование аварии или создание условий для возникновения аварийной ситуации. В результате возможно радиационное заражение местности и/или облучение персонала и населения.
* Кибератаки на автоматизированные системы СФЗ ЯО, включая систему физической защиты и систему учета и контроля ядерных материалов. В данном случае целью кибератаки может быть нарушение функционирования систем физической защиты и/или учета и контроля с целью подготовки хищения радиоактивных материалов или совершения диверсий, в том числе удаленное отключение средств контроля и управления доступом в помещениях с предметами защиты или изменение настроек измерительных систем, применяемых для учета и контроля ядерных материалов.
* Кибератаки на автоматизированные информационные системы ядерного объекта. Доступ, уничтожение или фальсификация данных дает злоумышленникам возможность осуществить хищение или диверсию, преодолеть меры СФЗ ЯО и т. П. В результате атаки могут быть изменены данные об инвентарных количествах ядерных материалов с целью сокрытия факта их хищения в течение как можно большего срока. Другой пример — несанкционированный доступ к системе документооборота ядерного объекта, где могут находиться сведения о графике проведения технического обслуживания элементов системы физической защиты, транспортирования ядерных материалов или порядке действий персонала по обнаружению и пресечению несанкционированных действий.