



КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ  
ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

1

# Защита уязвимых целей от террористических нападений

**РУКОВОДСТВО ПО ПЕРЕДОВОЙ ПРАКТИКЕ**

Вводный модуль



Глобальная программа по противодействию террористическим угрозам  
в отношении уязвимых целей

Осуществляется в партнерстве с:



UNITED NATIONS SECURITY COUNCIL  
COUNTER-TERRORISM COMMITTEE  
EXECUTIVE DIRECTORATE (CTED)



**UNAOC**  
United Nations Alliance of Civilizations



**unieri**  
United Nations  
International Crime and Justice  
Research Institute





КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ  
ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

# Защита уязвимых целей от террористических нападений

**РУКОВОДСТВО ПО ПЕРЕДОВОЙ ПРАКТИКЕ**

Вводный модуль

**Глобальная программа по противодействию террористическим угрозам  
в отношении уязвимых целей**

Осуществляется в партнерстве с:



UNITED NATIONS SECURITY COUNCIL  
COUNTER-TERRORISM COMMITTEE  
EXECUTIVE DIRECTORATE (CTED)



**UNAOC**  
United Nations Alliance of Civilizations



**unicri**  
United Nations  
Interregional Crime and Justice  
Research Institute



# Содержание

<b>Предисловие</b> .....	v
Указатель вставок .....	vii
Указатель конкретных примеров .....	vii
Указатель программных документов .....	viii
<b>1. Разъяснение базовых понятий</b> .....	1
1.1 Уязвимые, слабозащищенные и защищенные цели, места скопления людей и места общественного пользования .....	1
1.2 «Слабозащищенные цели» в сопоставлении с критически важными объектами инфраструктуры .....	3
<b>2. Террористическая угроза в отношении уязвимых целей</b> .....	6
<b>3. Уязвимость слабозащищенных целей перед террористическими нападениями</b> .....	9
<b>4. Смягчение рисков и реагирование: роли заинтересованных сторон</b> .....	11
4.1 Государства-члены .....	12
4.1.1 Обязательство государств-членов обеспечить учет прав человека и гендерного фактора в процессе противодействия террористическим угрозам для «слабозащищенных целей» .....	14
4.1.2 Лица, определяющие политику .....	15
4.1.3 Правоприменительная деятельность .....	28
4.1.4 Сотрудники служб экстренного реагирования .....	30
4.1.5 Разведывательные службы .....	32
4.2 Неправительственные субъекты .....	34
4.2.1 Операторы объектов .....	34
4.2.2 Организации гражданского общества .....	38
4.2.3 Частный сектор (кроме операторов объектов) .....	41
4.2.4 Пользователи уязвимых объектов .....	44
<b>Справочные материалы</b> .....	47





# Предисловие

В своем седьмом обзоре Глобальной контртеррористической стратегии Организации Объединенных Наций Генеральная Ассамблея Организации Объединенных Наций рекомендовала Контртеррористическому управлению Организации Объединенных Наций (КТУ ООН) и структурам Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности «тесно сотрудничать с государствами-членами и соответствующими международными, региональными и субрегиональными организациями для выявления и распространения передовых методов предотвращения террористических нападений на особо уязвимые цели, включая критически важные объекты инфраструктуры и общественные места («слабозащищенные цели»)».

Именно в этом контексте в рамках Глобальной программы КТУ ООН по противодействию террористическим угрозам в отношении уязвимых целей<sup>1</sup> был разработан настоящий документ, призванный служить вводным руководством по защите уязвимых объектов от террористических актов. В сочетании с четырьмя специальными тематическими модулями<sup>2</sup> он дополняет «Сборник передовых методов по защите критически важных объектов инфраструктуры от террористических атак»<sup>3</sup> с уделением особого внимания «слабозащищенным целям» как особому типу объектов, для обеспечения безопасности которых требуется особый подход со стороны широкого круга субъектов<sup>4</sup>.

Настоящий вводный модуль, в котором определяются основные понятия, обрисовывается широкая картина угроз и приводится обзор ролей и обязанностей заинтересованных сторон без указания конкретных секторов, создает основу для более глубокого и посекторального

1 Эта программа осуществляется Контртеррористическим управлением Организации Объединенных Наций (КТУ ООН), Исполнительным директором Контртеррористического комитета Организации Объединенных Наций (ИДКТК), Альянсом цивилизаций Организации Объединенных Наций (АЦ ООН) и Межрегиональным научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ). Она осуществляется в тесном взаимодействии с другими соответствующими организациями, включая Интерпол. URL: <https://www.un.org/counterterrorism/ru/vulnerable-targets>.

2 Четыре специальных модуля посвящены вопросам защиты религиозных и туристических объектов и городских центров, а также угрозам для уязвимых объектов в целом, исходящим от беспилотных авиационных систем.

3 Сборник был разработан в 2018 году в рамках Рабочей группы по защите критически важной инфраструктуры, в том числе уязвимых объектов, интернета и безопасности туризма, при Целевой группе Организации Объединенных Наций по осуществлению контртеррористических мероприятий (ЦГОКМ). В 2019 году ЦГОКМ вошла в структуры Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности (Договор). В рамках этой новой структуры рабочие группы ЦГОКМ по защите критически важной инфраструктуры, в том числе уязвимых объектов, интернета и безопасности туризма, и по предупреждению террористических нападений с применением оружия массового уничтожения и принятию ответных мер были объединены в Рабочую группу Договора по возникающим угрозам и защите критически важной инфраструктуры.

4 В настоящем документе и прилагаемых к нему специальных модулях используется терминологический подход, принятый Генеральной Ассамблеей Организации Объединенных Наций в связи с седьмым обзором Глобальной контртеррористической стратегии Организации Объединенных Наций. В частности, в резолюции 75/291 указывается, что «слабозащищенные цели» являются одной из двух подкатегорий уязвимых целей (вторая — «критически важные объекты инфраструктуры»).

изучения проблем и возможностей, связанных с защитой религиозных и туристических объектов и городских центров, а также применением беспилотных авиационных систем (БАС) для совершения террористических нападений на уязвимые цели.

Как вводный модуль, так и четыре специальных модуля содержат подборку конкретных примеров. Они наглядно демонстрируют, как ключевые принципы, связанные с вопросами безопасности, включая рекомендации, одобренные на международном уровне, используются на практике правительствами, организациями частного сектора, операторами уязвимых объектов и организациями гражданского общества. Кроме того, во всех модулях обобщается содержание нескольких программных документов (например, руководств, справочников, сборников), в которых приводятся директивы в отношении стратегий и оперативных действий, призванных уменьшить степень уязвимости объектов и повысить их устойчивость.

Приведенные в общем и специальных модулях аналитические рамки, конкретные примеры, программные документы и материалы являются результатом интенсивных камеральных исследований, официального запроса на представление материалов, направленного всем 193 государствам – членам Организации Объединенных Наций, обсуждений с отдельными экспертами, представителями международных организаций и партнерами по проектам, а также материалов, представленных Рабочей группой по возникающим угрозам и защите критически важной инфраструктуры Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности<sup>5</sup>. Важные выводы были сделаны в ходе серии онлайн-овых совещаний групп экспертов, которые были организованы в 2021 году КТУ ООН совместно с партнерами и в которых приняли участие национальные и международные эксперты и специалисты-практики из государств – членов Организации Объединенных Наций, международных и региональных организаций, групп гражданского общества, частного сектора и научных кругов. Кроме того, в этом процессе были использованы материалы, представленные Советником по гендерным вопросам КТУ ООН и специальным консультантом по правам человека КТУ ООН и Сектора специальных проектов и инноваций<sup>6</sup>.

---

5 <https://www.un.org/counterterrorism/ru/global-ct-compact>.

6 В настоящем документе и специальных модулях рассматривается необходимость учета гендерного фактора при разработке и осуществлении планов действий, а также необходимость разработки учитывающих гендерную специфику планов обеспечения безопасности, признания и поддержки роли женщин в обеспечении безопасности уязвимых целей, борьбы с гендерными предрассудками в правоприменительной сфере, учета гендерного фактора в подготовке специалистов, практической деятельности и проведении учений в рамках планов обеспечения безопасности и действий в чрезвычайных ситуациях, совместного решения особых проблем безопасности женщин в городских районах и устранения гендерных предрассудков в методах, используемых правоохранительными органами и службами безопасности. Этот перечень не является исчерпывающим, и на этапах от планирования до осуществления и оценки всех мер, указанных в различных модулях, необходимо учитывать контекстуальные соображения, касающиеся гендерного равенства.



## Указатель вставок

Вставка 1.	<b>Согласование усилий по защите «слабозащищенных целей» и критически важных объектов инфраструктуры</b>	5
Вставка 2.	<b>Защита мест общественного пользования: выводы Европейского совета</b>	13
Вставка 3.	<b>Государственно-частное партнерство (ГЧП) для защиты «слабозащищенных целей»</b>	19
Вставка 4.	<b>Расширенное понятие оперативной совместимости</b>	31
Вставка 5.	<b>Поощрение разработки планов обеспечения безопасности уязвимых целей с учетом гендерного фактора</b>	35
Вставка 6.	<b>Безопасность уязвимых объектов: взгляд оператора</b>	36
Вставка 7.	<b>Международный кодекс поведения частных охранных компаний</b>	43
Вставка 8.	<b>Средства «Facebook» для оказания помощи в реагировании на кризисы</b>	44
Вставка 9.	<b>Последствия для прав человека, порождаемые политикой и практикой, нацеленными на выявление признаков радикализации</b>	45



## Указатель конкретных примеров

Конкретный пример 1.	<b>Стратегия защиты мест скопления людей от терроризма, принятая в Австралии</b>	20
Конкретный пример 2.	<b>Обзор плана обеспечения безопасности «слабозащищенных целей» и мест скопления людей – Министерство внутренней безопасности Соединенных Штатов</b>	20
Конкретный пример 3.	<b>План «Вижипират», принятый во Франции</b>	25
Конкретный пример 4.	<b>Национальная система идентификации рисков, принятая Шведским гражданским агентством по чрезвычайным ситуациям</b>	27
Конкретный пример 5.	<b>Глобальный фонд для работы с населением и усиления его сопротивляемости</b>	40
Конкретный пример 6.	<b>Ликвидация травматических последствий терроризма: миссия Израильского центра травматологии и восстановительного лечения</b>	41



## Указатель программных документов

Программный документ 1.	<b>«слабозащищенных целей» — аналитическая справка ИДКТК</b>	15
Программный документ 2.	<b>Анталийский меморандум о защите «слабозащищенных целей» в контексте борьбы с терроризмом — Глобальный контртеррористический форум (ГКФ)</b>	16
Программный документ 3.	<b>Справочник по предупреждению терроризма и обеспечению готовности к нему — Международный центр по борьбе с терроризмом (МЦБТ)</b>	16
Программный документ 4.	<b>Справочник по вопросам создания государственно-частных партнерств для защиты уязвимых целей — ЮНИКРИ</b>	22
Программный документ 5.	<b>Анталийский меморандум: создание государственно-частных партнерств — ГКФ</b>	22
Программный документ 6.	<b>Предупреждение терроризма и борьба с насильственным экстремизмом и радикализацией, ведущими к терроризму: подход, основанный на взаимодействии полиции с населением — Организация по безопасности и сотрудничеству в Европе (ОБСЕ)</b>	29
Программный документ 7.	<b>Охрана общественного порядка и гендерный фактор — Женевский центр по управлению сектором безопасности, Бюро ОБСЕ по демократическим институтам и правам человека, Структура «ООН-женщины»</b>	30
Программный документ 8.	<b>Рамочный план реагирования на кризисные события и посткризисного восстановления — Министерство внутренней безопасности Соединенных Штатов</b>	31
Программный документ 9.	<b>Разведка и гендерный фактор — Женевский центр по управлению сектором безопасности, Бюро ОБСЕ по демократическим институтам и правам человека, Структура «ООН-женщины»</b>	33
Программный документ 10.	<b>Избранные ресурсы для операторов объектов, представляющих собой уязвимые цели, — Министерство внутренней безопасности Соединенных Штатов</b>	36
Программный документ 11.	<b>Избранные ресурсы для пользователей объектов, представляющих собой уязвимые цели, — Министерство внутренней безопасности Соединенных Штатов</b>	46



# Разъяснение базовых понятий

## 1.1 Уязвимые, слабозащищенные и защищенные цели, места скопления людей и места общественного пользования



Понятия уязвимые, слабозащищенные и защищенные цели, места скопления людей и места общественного пользования лишь недавно стали широко использоваться в тематике противодействия терроризму<sup>7</sup>. Более того, их определения не включены ни в одну международно-правовую базу. В определенной степени их значение меняется в зависимости от кон-

текста и характера обсуждения (политического, правового, оперативного и технического), в котором они используются.

В соответствии с принятой в июне 2021 года резолюцией Генеральной Ассамблеи Организации Объединенных Наций об обзоре Глобальной контртеррористической стратегии, в настоящем документе и

<sup>7</sup> Генеральная Ассамблея Организации Объединенных Наций впервые упомянула «уязвимые цели» в 2006 году. В рамках Глобальной контртеррористической стратегии Организации Объединенных Наций и ее плана действий по компоненту II «Меры по предупреждению терроризма и борьбе с ним» государства-члены обязались «активизировать все усилия по укреплению безопасности и защиты особо уязвимых объектов, таких как объекты инфраструктуры и места общественного пользования».

соответствующих специальных модулях учитывается, что к уязвимым целям относятся критически важные объекты инфраструктуры и «слабозащищенные цели»<sup>8</sup> (A/RES/75/291) и что их защита должна обеспечиваться путем применения подходов, учитывающих гендерный фактор и соответствующих правам человека<sup>9</sup>.

В широком смысле под «слабозащищенными целями» понимаются такие виды уязвимых объектов, как стадионы, торговые центры, театры, религиозные учреждения, пешеходные зоны, которые легко доступны и открыты для общественности и по этим причинам намеренно не предусматривают никаких мер обеспечения безопасности или предусматривают ограниченные меры. Эта особенность, в сочетании с большим скоплением людей, которое часто отмечается в этих местах, делает их привлекательными целями для террористов, стремящихся вызвать массовые жертвы и/или масштабные разрушения таким образом, чтобы для этого не требовалось масштабного планирования и подготовки или значительных ресурсов, но чтобы это вызвало несоразмерно большое освещение в средствах массовой информации<sup>10</sup>. Понятие «слабозащищенные цели» не поддается точному определению еще и потому, что места, которые обычно ассоциируются с ним, являются крайне неоднородными. «Слабозащищенными целями» могут быть крытые или открытые объекты постоянного или временного характера. Они могут иметь различные размеры, функции, физические характеристики, местоположение и профили пользователей.

«Слабозащищенность» одних объектов контрастирует с «защищенностью» других. Политики, военные и сотрудники правоохранительных органов рассматривают «слабозащищенные цели» в сопоставлении с «защищенными целями». К последним относятся объекты, которые обычно обслуживаются или часто посещаются правительственными должностными лицами и защищены надежными мерами обеспечения физической безопасности (например, посольства, военные объекты, места проведения встреч на высшем уровне).

В значительной мере понятие «слабозащищенные цели» пересекается с понятием «места скопления людей». В понятии «места скопления людей» подчеркивается высокая плотность людей, собирающихся в определенных местах и вокруг них (например, посетители туристического объекта, зрители на концерте, прихожане на религиозной церемонии), в качестве особого фактора уязвимости или привлекательности для враждебно настроенных субъектов. Понятие «слабозащищенные цели» также часто используется как синоним понятия «места общественного пользования», хотя не все места общественного пользования обязательно (или всегда) являются местами скопления людей, а места скопления людей не обязательно являются общественными или особо уязвимыми местами (например, когда несколько человек участвуют в мероприятии в строго охраняемом правительственном здании).

---

8 В указанных модулях основное внимание уделяется «слабозащищенным целям», а не на защите критически важных объектов инфраструктуры, поскольку последние подробно рассматриваются в опубликованном в 2018 году издании «Защита критически важных объектов инфраструктуры от террористических атак: сборник передового опыта», URL: [https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium\\_of\\_good\\_practices\\_ru.pdf](https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf).

9 В разделе 3.1 представлен обзор обязательств государств-членов по обеспечению соответствия любых принимаемых ими мер для противодействия терроризму всем их обязательствам по международному праву, в частности, международному праву прав человека и, в контексте настоящего документа, их учету при разработке и реализации мер по защите «слабозащищенных целей».

10 Как подчеркнул Контртеррористический комитет Совета Безопасности Организации Объединенных Наций, «привлекательность “слабозащищенных целей” для террористов обусловлена не только их открытостью и ограниченностью принимаемых мер охраны и безопасности, что облегчает доступ к ним, но и потенциальной возможностью жертв среди гражданского населения, хаоса, широкого общественного резонанса и экономических последствий» (S/2018/1177, пункт 51).

## 1.2 «Слабозащищенные цели» в сопоставлении с критически важными объектами инфраструктуры



Понятие «слабозащищенная цель» обычно отделяют от понятия «критически важный объект инфраструктуры», хотя последний может быть «слабозащищенным» в силу отсутствия надлежащих мер обеспечения защиты. Критически важные объекты инфраструктуры в широком смысле обозначают объекты, системы и процессы, которые имеют жизненно важное значение для обеспечения основных услуг (например, здравоохранение, водоснабжение, телекоммуникации, транспорт, энергоснабжение), и нарушение ра-

боты которых может вызвать широкие негативные последствия<sup>11</sup> для безопасности и социального и экономического благополучия населения<sup>12</sup>.

Ключевые элементы, определяющие различия, включают следующее:

- «слабозащищенная цель» обычно представляет собой физический объект, в то время как критически важная инфраструктура может включать и процессы, в том числе информационные системы и сети<sup>13</sup>;

11 Строго говоря, туристический сектор обычно не относится к числу критически важных секторов, однако в некоторых государствах-членах он может обеспечивать весьма значительную долю национального ВВП. Когда террористические акты затрагивают страны, экономика которых в значительной степени зависит от туризма, общие финансовые и социальные последствия могут равняться последствиям, вызванным крахом критически важного сектора, или превосходить их.

12 В *Сборнике передового опыта* по защите критически важных объектов инфраструктуры от террористических атак приводятся несколько национальных определений «критически важных объектов инфраструктуры». Кроме того, в нем рассматриваются методологии, используемые странами для определения секторов и объектов, которые должны считаться критически важными (раздел 2.4.1, Определение «критичности», с. 32).

13 Понятие критически важной информационной инфраструктуры имеет ключевое значение для понимания той роли, которую играют компьютеризированные системы в управлении работой электростанций, плотин, мостов, цепочек поставок продовольствия и т. д.

- определяющей чертой «слабозащищенных целей» является их открытость и доступность для населения. В отличие от них критически важные объекты инфраструктуры, как правило, закрыты для посторонних<sup>14</sup>;
- в основе обеспечения защиты «слабозащищенных целей» и критически важных объектов инфраструктуры лежат различные соображения. Критически важные объекты инфраструктуры находятся под защитой на том основании, что они составляют основу жизни стран, а также в силу того, что сбой в одном секторе могут повлечь за собой «каскадный эффект» в других секторах и потенциально вызвать общий коллапс. Это объясняет, почему усилия по защите критически важных объектов инфраструктуры, в отличие от усилий по защите «слабозащищенных целей», призваны оградить их не только от риска террористических нападений, но и от последствий других действий человека (преднамеренных или совершенных по неосторожности), а также, что особенно важно, от разрушительного воздействия природных явлений.

Эти концептуальные различия означают, что институциональные и нормативные рамочные основы, необходимые для защиты критически важных объектов инфраструктуры, могут и не применяться автоматически к «слабозащищенным целям». Это видно из критериев, используемых государствами-членами для проведения различий между критически важными и некритически важными объектами инфраструктуры. Эти критерии, которые часто основываются на моделях прогнозирования степени серьезности, продолжительности, географического охвата и экономических последствий пагубных событий, могут не подходить для определения понятия «слабозащищенных целей».

Вместе с тем, несмотря на имеющиеся различия, обеспечение защиты «слабозащищенных целей» и критически важных

объектов инфраструктуры сопряжено с множеством общих проблем, в связи с чем можно сделать вывод о том, что оба эти аспекта должны выиграть от принятия изложенного ниже синергического подхода:

- меры, разработанные для защиты критически важных объектов инфраструктуры, могут послужить ценным источником вдохновения для защиты «слабозащищенных целей» и наоборот. На базовом уровне многие средства обеспечения физической безопасности, используемые для контролирования доступа на критически важные объекты инфраструктуры (например, посты охраны, заборы, металлодетекторы), как правило, также используются для регулирования доступа населения к «слабозащищенным целям»<sup>15</sup>;
- способ, примененный для управления нападением на критически важный объект инфраструктуры, может послужить полезным предупреждением и уроком в усилиях по предотвращению и уменьшению рисков и урегулированию кризисов, связанных со «слабозащищенными целями»;
- защита как критически важных объектов инфраструктуры, так и «слабозащищенных целей» основана на необходимости применения операторами объектов и государственными органами подходов, предусматривающих управление рисками и регулирование кризисов. Процедуры и соответствующие институциональные структуры, задействуемые в национальной оценке угроз и реагировании на нападения на критически важные объекты инфраструктуры и «слабозащищенные цели», часто полностью совпадают или в значительной степени пересекаются. Кроме того, в большинстве случаев критически важные объекты инфраструктуры и «слабозащищенные цели» находятся в частном владении и управлении, что делает развитие государственно-частного партнерства (ГЧП) од-

14 Закрытость критически важного объекта инфраструктуры для населения не означает, что этот объект защищен лучше, чем «слабозащищенные цели». В отсутствие адекватных мер обеспечения безопасности критически важные объекты инфраструктуры могут быть крайне уязвимыми и, следовательно, особенно привлекательными для террористов.

15 Другие примеры мер обеспечения безопасности, которые можно с пользой использовать для защиты как критически важных объектов инфраструктуры, так и «слабозащищенных целей», можно найти в концепции «умного города» и связанных с ней технологических решениях, призванных усилить безопасность современных городов. Например, цифровые датчики, предназначенные для обнаружения оружия, вполне можно использовать для обеспечения безопасности таких различных объектов, как уличные рынки, правительственные здания или транспортная система.

ним из центральных элементов усилий по обеспечению готовности и защиты и тех, и других;

- взаимодействие между защитой критически важных объектов инфраструктуры и «слабозащищенных целей» носит многоплановый характер и требует тесной политической, институциональной и оперативной координации. Критически важная инфраструктура — это то, что в большинстве случаев позволяет функционировать «слабозащищенным целям». Например, для проведения спортивного мероприятия необходима бесперебойная подача электроэнергии. В то же время, срыв предоставления таких основных услуг, как электроснабжение, может не просто оставить присутствующих в концертном зале в темноте и прервать выступление, но и потенциально может являться частью стратегии, призванной затруднить эва-

куацию во время террористического нападения. При этом успешное террористическое нападение на многолюдный туристический или религиозный объект может вызвать разрушение критически важного объекта инфраструктуры и даже целого критически важного сектора. Например, больницы могут быстро переполниться, а коммуникационные сети, перегруженные запросами пользователей, перестанут работать. Нападения на «слабозащищенные цели» могут иметь особенно серьезные последствия для критически важных объектов инфраструктуры, когда они происходят в городских районах, где эти цели и объекты соседствуют и взаимодействуют в сложных и густонаселенных пространствах, что обуславливает необходимость применения подхода, в котором они рассматриваются как часть единой многогранной системы.



Вставка 1.

### **Согласование усилий по защите «слабозащищенных целей» и критически важных объектов инфраструктуры**

«Такие критически важные объекты инфраструктуры, как электросети, плотины и правительственные объекты, по-прежнему будут оставаться в списке целей террористов. Во многих странах «слабозащищенные цели» нередко являются частью системы критически важной инфраструктуры. Поэтому в системе управления рисками для инфраструктуры также учитывается угроза в отношении «слабозащищенных целей». Например, нападения на людей на железнодорожной станции являются частью комплекса потенциальных сценариев нападения на транспортные системы (например, воздушные, железнодорожные, морские). Многие из ключевых принципов, которых придерживаются правительства при обеспечении защиты критически важных объектов инфраструктуры от террористических актов, также могут быть эффективны для защиты «слабозащищенных целей»... Как обеспечение защиты «слабозащищенных целей», так и обеспечение безопасности и способности к восстановлению нормального функционирования критически важных объектов инфраструктуры требуют одинаковых основных политических и практических рамок для обеспечения готовности, т. е. предотвращения, защиты, смягчения последствий, реагирования и восстановления. Эти усилия должны быть взаимодополняющими... Оценки «слабозащищенных целей» должны проводиться совместно с оценкой возможностей государственных ведомств по разработке планов и созданию партнерств для защиты критически важных объектов инфраструктуры. В ряде случаев «слабозащищенные цели» могут совпадать с критически важными объектами инфраструктуры (коммерческие объекты), а в некоторых случаях могут и не совпадать (энергетический сектор)».

*Источник:* Анталийский меморандум, 2017 год, пример передовой практики № 5.



## Террористическая угроза в отношении уязвимых целей

В последние несколько лет спецслужбы и правоохранительные органы по всему миру регулярно обращали внимание на наличие постоянной террористической угрозы в отношении мест массового скопления людей. Во многих случаях население в целом осведомлено об этой угрозе, поскольку террористические организации публично призывали к совершению нападений или угрожали нападениями на такие места<sup>16</sup>.

Не исключено, что террористы могут переключить свое внимание на «слабозащищенные цели» в ответ на усиление мер безопасности, которые усложняют совершение нападений на такие «защищенные цели», как правительственные здания, военные объекты и т. д. Ситуацию можно сравнить с «эффектом воздушного шара», когда усиление деятельности по охране правопорядка и обеспечению безопасности в определенных географических районах может привести к перемещению той же самой криминогенной проблемы в менее эффективно охраняемые районы. В этом же ключе следует отметить, что после того, сектор гражданской авиа-

ции прореагировал на террористическую угрозу путем введения все более жестких мер обеспечения безопасности в предпосадочных зонах, террористические группы переключили свое внимание на соседние, менее защищенные зоны<sup>17</sup>.

В то же время, как подчеркивается в Анталлийском меморандуме Глобального контртеррористического форума, «недавний рост числа нападений с применением ножей и тяжелых транспортных средств, в отличие от нападений, совершаемых вооруженными людьми или группами боевиков, иногда сопровождаемых террористами-смертниками, свидетельствует о проявлении гибкости и о готовности согласиться на меньшее число жертв»<sup>18</sup>.

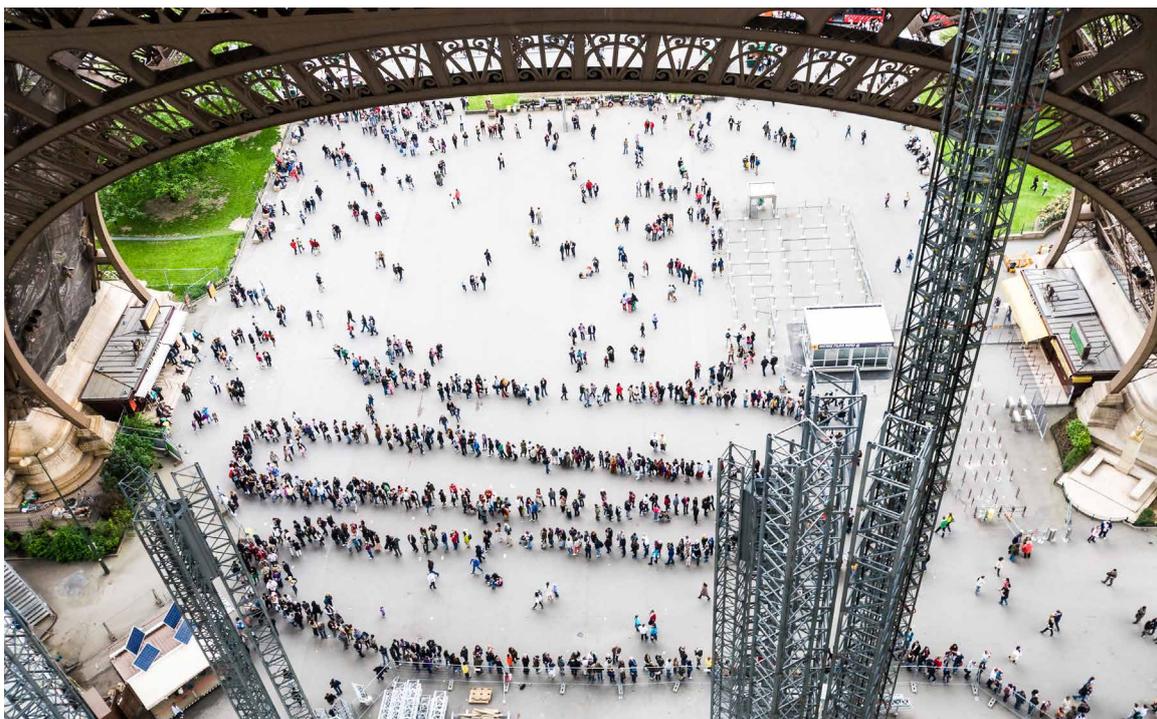
Хотя оружие, которое применялось в ряде недавних нападений, было примитивным, нельзя исключать вероятность применения террористами оружия массового уничтожения против «слабозащищенных целей». Самой известной попыткой такого рода является нападение с применением газа зарин, совершенное террористической группой «Аум синрикё» в 1995 году в токийском метро<sup>19</sup>.

16 Например, в ноябре 2016 года «Исламское государство» разместило в своем интернет-журнале обращенный к своим сторонникам призыв нападать на такие объекты, как места проведения крупных собраний и празднеств под открытым небом, многолюдные улицы, открытые рынки, места проведения фестивалей, парадов и политических митингов.

17 Такая точка зрения убедительно подтверждается террористическим актом, который произошел в Брюсселе в 2016 году. Нанося удар в зоне регистрации аэропорта, до прохождения контроля безопасности, террористы выбирают место, заполненное пассажирами и чемоданами, что позволяет им свести риск срыва своего плана к минимуму и одновременно максимально увеличить шансы нанести значительный ущерб.

18 Особую угрозу представляют начиненные взрывчаткой автомобили, которые могут быть припаркованы и взорваны вблизи «слабозащищенных целей». С самого начала многие террористические группы использовали для этих целей машины скорой помощи, которые выглядят вполне безобидно.

19 Менее известный инцидент произошел в 1984 году, когда группа лиц, которые пытались повлиять на местные выборы, намеренно заразила сальмонеллой салат-бары в десяти ресторанах штата Орегон, Соединенные Штаты. Этот инцидент показывает, сколь относительно легко враждебно настроенные субъекты могут потенциально совершить биотеррористическое нападение на «слабозащищенную цель».



Кроме того, террористические акты, направленные против «слабозащищенных целей» продолжают совершаться в целях захвата заложников<sup>20</sup>, и потенциально под прицелом террористов могут оказаться места, в которых можно получить опасные материалы для использования в террористических целях в других местах<sup>21</sup>.

На характер и уровень угрозы в отношении «слабозащищенных целей» влияют местные факторы, а также особенности воинственно настроенных субъектов, которые стремятся нанести ущерб таким объектам и находящимся на них людям. Выбор террористами того или иного объекта для нападения зависит от целого ряда соображений, таких как личная обида на определенные группы (например, на определенные религиозные общины, туристов из определенных стран, представления об аморальном характере той или иной деятельности) и фактическая или предполагаемая степень уязвимости объектов. Как

правило, террористы могут принимать решения о совершении нападений на «слабозащищенные цели» по целому ряду причин<sup>22</sup>. В дополнение к мотивам, которые обычно ассоциируются с решениями нанести удар по уязвимым объектам (например, наличие большого скопления людей в сочетании со слабыми мерами безопасности или их отсутствием, близость к зоне деятельности группы или наличие доступа, возможность оперативного освещения в средствах массовой информации), могут существовать и другие мотивы, включающие следующее:

- компенсация собственной слабости: если террористическая группа и/или террорист-одиночка не имеет ресурсов или возможностей планирования для проведения успешного нападения на «защищенную цель», то они могут переключиться на «слабозащищенную цель»;

20 Например, после захвата 850 человек в заложники в московском театре на Дубровке террористы в качестве условия их освобождения выдвинули конкретные политические требования к российскому правительству. На северо-западе Нигерии частые массовые похищения девочек и мальчиков в школах-интернатах, как правило, совершаются с целью получения выкупа.

21 В докладе правительства Соединенных Штатов за 2012 год отмечается отсутствие надлежащих мер безопасности в ряде медицинских учреждений, в которых хранятся радиоактивные материалы, и содержится предупреждение о том, что враждебно настроенные субъекты могут воспользоваться лазейками в системе безопасности, чтобы похитить такие материалы и собрать «грязную бомбу». (GAO 2012)

22 Hesterman 2019, *Soft Target Hardening*, p.23-26.



- выбор цели в качестве последнего варианта: террористическая группа, частично утратившая свою привлекательность и/или оперативные возможности, может обратить свое внимание на уязвимые «слабозащищенные цели», чтобы восстановить репутацию и привлечь новых сторонников в свои ряды;
- тестирование новой стратегии, тактики или оружия: «слабозащищенные цели» могут использоваться в качестве полигона для подготовки к «более значительным» операциям;
- наличие возможностей для проявления гибкости: «слабозащищенные цели» могут обеспечивать более широкие возможности для импровизации в случае, если по каким-либо причинам возникнет необходимость внести изменения в первоначальный план.



## Уязвимость слабозащищенных целей перед террористическими нападениями

Каждый тип объекта имеет свой уникальный набор факторов уязвимости, обусловленных в значительной мере особенностями лиц, которые управляют таким объектом, эксплуатируют или посещают его, и ресурсами, которые доступны таким лицам. Например, в большинстве религий и религиозных общин закреплена обязанность проводить политику «открытых дверей», которая заключается в том, что они приветствуют посторонних и не задают вопросов о личности или происхождении неизвестных посетителей. Кроме того, при совершении нападений преступники могут использовать «эффект внезапности», особенно когда служители культа погружены в совершение культового обряда. В положительном ключе можно отметить тот факт, что регулярные посетители религиозных объектов могут лучше знать расположение эвакуационных путей и аварийных выходов по сравнению с теми, кто впервые оказался на туристическом объекте.

Кроме того, степень уязвимости значительно варьируется в зависимости от социально-экономических условий, географического положения и окружающей местности, а также физических характеристик объекта. Например, рынок под открытым небом может быть сложнее атаковать путем выброса отравляющих веществ, чем какой-нибудь закрытый объект, например театр. В тоже время зрители театра значительно меньше подвержены действиям беспилотников, чем посетители уличного рынка.

Несмотря на имеющиеся различия, можно выделить ряд факторов уязвимости, которые, как представляется, широко присут-

ствуют в различных секторах и коренятся в культурных, институциональных, правовых и финансовых особенностях:

- *человеческий фактор*: уязвимость может возникнуть вследствие нежелания проводить необходимую модернизацию системы безопасности по причине недооценки вероятности и/или последствий террористического нападения. Позиция некоторых владельцев/операторов объектов может быть следствием «сопротивления изменениям», то есть готовности пожертвовать надежной системой безопасности в угоду созданию более благоприятного впечатления для верующих, туристов, посетителей торговых центров, культурных мероприятий и т. д. Другим потенциально значимым фактором является «усталость от безопасности»: после периодов сохранения повышенной бдительности, к которой призывают власти после террористического нападения, часто возникает проблема сохранения культуры безопасности в качестве долгосрочной программы для операторов объектов, общественности и других заинтересованных сторон. Сами лица, ответственные за обеспечение безопасности, могут вызывать подозрения или получать плохой прием в определенных сообществах (например, в некоторых религиозных общинах).

Кроме того, конкретные факторы уязвимости могут быть результатом появления культурных барьеров, обусловленных различиями в жизненном опыте, ожиданиях и менталитете тех или иных заинтересованных лиц, призванных со-

трудничать в деле защиты уязвимых объектов, и связанного с этими барьерами нежелания принимать более жесткие меры безопасности, что делает создание эффективных государственно-частных партнерств (ГЧП) критически важной, но в то же время сложной задачей<sup>23</sup>;

- *институциональные и правовые факторы*: хотя обмен информацией является существенно важным компонентом любой эффективной системы управления рисками и регулирования кризисов, призванной обеспечивать защиту уязвимых объектов, практическое решение этой императивной задачи может быть затруднено недостаточной межведомственной координацией вследствие пробелов в нормативно-правовом регулировании, отсутствия четкого распределения обязанностей и т. д. Кроме того, спецслужбы могут сталкиваться препятствиями юридического характера при раскрытии секретной информации операторам уязвимых объектов.

На местах могут возникать недоразумения в отношениях между арендодателями и арендаторами уязвимых объектов, а также между операторами объектов и соседними коммерческими структурами по поводу того, кто должен отвечать за модернизацию систем безопасности или управление персоналом службы безопасности на так называемой «серой территории», т. е. в

спорных помещениях или помещениях, не имеющих четко определенного владельца. Это может повлечь за собой непринятие мер обеспечения безопасности, необходимых в превентивных целях, и потенциально может снизить эффективность мер, принимаемых после инцидента;

- *факторы, связанные с наличием ресурсов*: многие уязвимые объекты имеют ограниченный бюджет для целей обеспечения безопасности. Принятие мер обеспечения безопасности может быть сопряжено с большими расходами, если для этого потребуется внести физические изменения или дополнительные элементы в объекты инфраструктуры, нанять новые охранные компании или провести подготовку персонала. Кроме того, операторы объектов могут и не иметь доступа к финансовым стимулам (например, денежным выплатам, субсидиям или налоговым льготам) в поддержку модернизации систем безопасности. Например, в условиях жестких бюджетных ограничений уязвимые объекты могут сделать выбор в пользу инвестирования скудных ресурсов в быстро окупаемые маркетинговые операции, а не в долгосрочный ремонт систем безопасности, что не даст возможности ликвидировать факторы уязвимости, которыми вполне могут воспользоваться злоумышленники.

---

23 Иногда государственные органы могут обращаться к операторам объектов с бескомпромиссными требованиями провести дорогостоящие работы по усилению безопасности. В свою очередь, операторы объектов, находящихся в частной собственности, могут проявлять нерешительность в плане участия в создании прочных и долговечных ГЧП вследствие таких факторов, как неспособность увидеть коммерческую ценность ГЧП, подозрительность в отношении мотивов государственного сектора и нехватка стимулов в силу отсутствия нормативных требований к участию частного сектора.



## Смягчение рисков и реагирование: роли заинтересованных сторон



Основополагающей парадигмой для целей защиты уязвимых целей от террористических актов, независимо от типа, размера или функции объекта, является скоординированное планирование мер обеспечения безопасности на основе подхода к управлению рисками и регулированию кризисов, применяемого операторами объектов и государственными властями как на национальном, так и на местном уровне.

Управление рисками определяется Управлением Организации Объединенных Наций по снижению риска бедствий (УСРБ ООН) как «систематический подход и практика

управления факторами неопределенности в целях минимизации потенциального ущерба и потерь. Управление рисками включает в себя оценку и анализ рисков, а также реализацию стратегий и конкретных действий по контролю, уменьшению и передаче рисков».

Нельзя недооценивать важность обеспечения тесной координации подходов к управлению рисками с участием всех уровней власти и других соответствующих субъектов. Генеральная Ассамблея Организации Объединенных Наций<sup>24</sup> «... рекомендует государствам-членам рас-

<sup>24</sup> См. Международную стратегию уменьшения опасности бедствий, Терминологический глоссарий по снижению риска бедствий, 2009 год.

смотреть возможность разработки или дальнейшего совершенствования своих стратегий уменьшения рисков террористических нападений на критически важные объекты инфраструктуры — стратегий, которые должны предусматривать, в частности, оценку и улучшение понимания соответствующих рисков, принятие мер по обеспечению готовности, в том числе эффективного реагирования на такие нападения, а также содействие повышению оперативной совместимости в области безопасности и ликвидации последствий и поддержку эффективного взаимодействия всех заинтересованных сторон». Кроме того, как подчеркивается в Антальском меморандуме ГКФ, «данные для оценки рисков могут поступать из различных источников. Национальные оценки, проводимые правительственными экспертами по безопасности, будут включать в себя чувствительную и секретную информацию, доступную только официальным представителям страны. После этого они должны быть объединены с информацией из открытых источников и информацией от отраслевых кругов и частного сектора в форме, доступной для местных сил безопасности, которые в ней нуждаются. Как государственный, так и частный сектор используют анализ рисков для выявления и

смягчения факторов уязвимости физической инфраструктуры, а также в своих постоянно действующих инструкциях и планах реагирования».

Что касается регулирования кризисов, то в широком смысле это понятие относится к процессам, которые необходимо задействовать в случае инцидента. Три основных этапа регулирования кризисов включают разработку планов действий на случай нештатных/чрезвычайных ситуаций, выявление кризиса, а также принятие антикризисных мер и урегулирование кризиса<sup>25</sup>.

В приведенных ниже разделах приводится краткий обзор ролей, которые отдельные заинтересованные стороны могут и должны играть в защите уязвимых целей в системе управления рисками и регулирования кризисов. Тот же подход, основанный на участии заинтересованных сторон, применяется в специальных модулях, в которых рассматривается вопрос о том, каким образом правительственные и неправительственные субъекты могут внести конкретный вклад в дело защиты религиозных и туристических объектов, городских центров, а также уязвимых объектов в целом от применения террористами беспилотных авиационных систем (БАС).

## 4.1 Государства-члены

Все уровни власти должны быть вовлечены в защиту уязвимых целей на основе их соответствующих сфер компетенции в рамках законодательной системы отдельных стран.

На базовом уровне общие контртеррористические меры представляют собой набор инструментов, которые должны быть определены заранее. Необходимо использовать весь набор инструментов и стратегий по борьбе с терроризмом в полном соответствии с правами человека, стандартами гендерного равенства и применимыми нормами международного права. К ним относятся принятие мер по противодействию насильственному экстремиз-

му; разработка и внедрение комплексных и специализированных стратегий уголовного преследования, реабилитации и реинтеграции; предотвращение доступа террористов к оружию; задействование основанных на международных договорах механизмов международного сотрудничества и обмена информацией, обеспечение охраны границ и управления границами в целях предотвращения трансграничного перемещения террористов и пресечения потока иностранных боевиков-террористов; и пресечение потока товаров, включающих предметы двойного назначения (например, для изготовления самодельных взрывных устройств).

25 В Сборнике передового опыта по защите критически важных объектов инфраструктуры от террористических атак содержатся дополнительная информация и рекомендации по управлению рисками и регулированию кризисов, которые в равной степени применимы к усилиям по защите критически важных объектов инфраструктуры и «слабозащищенных целей» (см. раздел 2.6 Сборника).

В приведенных ниже подразделах изложены ключевые роли и обязанности по защите уязвимых целей в рамках политического и правоприменительного потенциала

стран, а также по поддержке контртеррористических усилий посредством сбора и анализа разведывательной и иной информации.



Вставка 2.

### **Защита мест общественного пользования: выводы Европейского совета**

В июне 2021 года Совет Европейского союза (правосудие и внутренние дела) принял ряд адресованных государствам – членам Европейского союза рекомендаций по защите мест общественного пользования от террористических актов. В приведенном ниже перечне кратко изложены ключевые аспекты:

- работать в направлении внедрения или совершенствования национальных, а также региональных и местных стратегий повышения устойчивости местных сообществ и мест общественного пользования;
- поддерживать инициативы по созданию надежной оперативной и унифицированной системы связи Европейского союза для правоохранительных органов и других специалистов-практиков по вопросам безопасности, чтобы иметь возможность обеспечивать надлежащую защиту и реагирование в случаях, требующих трансграничного сотрудничества в отношении мест общественного пользования, и при проведении крупных мероприятий;
- изучить национальные нормативно-правовые базы с целью ограничения незаконного ношения холодного оружия в местах общественного пользования и на крупных мероприятиях;
- изучить и проанализировать директивные указания и инструменты по обеспечению безопасности для операторов проката автомобилей с целью предотвращения и смягчения риска совершения нападений в местах общественного пользования с использованием автомобилей;
- проанализировать внутреннее законодательство и местные нормативные акты на предмет проверки наличия в них четких положений, определяющих административные требования и обязанности для субъектов, отвечающих за планирование и обеспечение безопасности в местах общественного пользования;
- продолжать планировать и организовывать практические учения и совместную подготовку с участием местных органов власти, правоохранительных органов, сил гражданской обороны, скорой медицинской помощи, частных коммерческих структур, частных охранных фирм и других заинтересованных сторон с целью повышения степени готовности и отработки методов реагирования правоохранительных органов и аварийно-спасательных служб;
- внедрять методы предупреждения преступности посредством среднего проектирования на местном уровне и в рамках государственно-частных партнерств и проектов в качестве механизма защиты мест общественного пользования, а именно для предотвращения использования автомобилей в качестве таранного средства, взрывов, применения химического, биологического, радиологического или ядерного оружия (ХБРЯ), самодельных зажигательных устройств и огнестрельного оружия, а также совершения других действий в таких местах, как железнодорожные станции и станции метро, общественные зоны международных аэропортов, культовые объекты, коммерческие зоны, туристические объекты (например, памятники и музеи), университеты, школы и другие места, которые могут быть определены по результатам оценки рисков.

Источник: <https://data.consilium.europa.eu/doc/document/ST-9545-2021-INIT/en/pdf>

#### 4.1.1 Обязательство государств-членов обеспечить учет прав человека и гендерного фактора в процессе противодействия террористическим угрозам для «слабозащищенных целей»

Терроризм представляет серьезную угрозу не только для международного мира и безопасности, но и для осуществления прав человека и для социально-экономического развития. Государства-члены принимают меры по эффективному противодействию терроризму и его предотвращению в рамках своих обязательств по международному праву прав человека, касающихся защиты права на жизнь и личную безопасность. Это обязательство особенно важно в свете потенциальных последствий нападений на «слабозащищенные цели» для населения, особенно с учетом открытости и доступности таких объектов, в которых скапливается большое количество людей.

Обязанность государств защищать права человека подразумевает обязательство принимать необходимые и адекватные меры для предотвращения и пресечения таких угрожающих этим правам действий, как угрозы национальной безопасности или насильственные преступления, включая терроризм, и для наказания за их совершение. В этом отношении государства должны руководствоваться, в частности, Глобальной контртеррористической стратегией Организации Объединенных Наций, в которой подчеркивается, что эффективная борьба с терроризмом и обеспечение соблюдения прав человека являются не взаимоисключающими, а взаимодополняющими и взаимоусиливающими целями. Действительно, поощрение и защита прав человека представляют собой самостоятельный основной элемент, который непременно должен присутствовать во всех аспектах деятельности по обеспечению успешной реализации всех четырех компонентов Стратегии. Совет Безопасности Организации Объединенных Наций также последовательно и неоднократно заявлял, что государства-члены должны обеспечивать, чтобы любые меры, принимаемые в целях борьбы с терроризмом, согласовывались со всеми их обязательствами по международному праву, в частности международному праву прав человека, между-

народному беженскому праву и международному гуманитарному праву. Более того, в своей резолюции 2178 (2014) Совет Безопасности заявил, что невыполнение этих и других международных обязательств, в том числе обязательств, закрепленных в Уставе Организации Объединенных Наций, является одним из факторов, способствующих все большей радикализации.

Следует также отметить, что, как предусматривается соответствующими положениями резолюций Совета Безопасности Организации Объединенных Наций, любые принимаемые меры по предупреждению терроризма и борьбе с ним должны соответствовать обязательствам государств по международному праву, в частности международному праву прав человека, международному беженскому праву и международному гуманитарному праву. Контртеррористические стратегии должны учитывать также гендерные и возрастные особенности, наилучшие интересы ребенка и фактор дифференцированного воздействия терроризма и насильственного экстремизма, служащего питательной средой для терроризма, на права человека женщин и девочек (см. S/2018/1177, приложение, п. 8).

В целях пресечения террористических угроз в отношении «слабозащищенных целей» государственные органы могут на временной основе принимать меры, которые могут привести к ограничению определенных прав, при условии, что такие ограничения соответствуют условиям, предусмотренным нормами международного права прав человека. Такие меры должны быть реальным ответом на наличную угрозу, должны быть вызваны требованиями ситуации, иметь четкую правовую основу и не выходить за рамки того, что необходимо для достижения законных целей. Государства должны обеспечить предоставление удовлетворительных гарантий для защиты от произвольного и несоразмерного ограничения прав человека в этом контексте. Чтобы обеспечить реальное выполнение этих обязательств государствам настоятельно рекомендуется регулярно проводить оценку мер, принимаемых для борьбы с террористической угрозой в отношении «слабозащищенных целей», с точки зрения соблюдения прав человека и обеспечивать, чтобы такие меры основывались на фактических дан-

ных и, следовательно, были эффективными, не усиливали отчуждение, предрассудки или предубеждения, не препятствовали доступу к объектам или их использованию для определенных групп или слоев населения. В том же ключе следует отметить что, учет гендерного фактора в деятельности по защите уязвимых целей является неотъемлемой частью эффективных и действенных стратегий смягчения рисков, поскольку это позволяет учесть не только гендерно дифференцированные потребности женщин, мужчин, мальчиков и девочек в плане безопасности, но и то, как подспудные гендерные отношения, стереотипы и динамика влияют на модели безопасности или ее отсутствия и факторы уязвимости.

#### 4.1.2 Лица, определяющие политику

В рамках параметров, установленных общей государственной стратегией, отдельные министерства и ведомства должны планировать свое участие, исходя из особенностей объектов, за которые они несут политическую, нормативную, инспекционную или иную ответственность. Кроме того, необходимо будет наладить партнерские отношения с различными категориями

заинтересованных сторон. Например, если для обеспечения защиты религиозных объектов требуется постоянный диалог с религиозными лидерами, то для предотвращения террористических нападений на туристические объекты необходимо задействовать туристическую индустрию. В то время как безопасность уязвимых городских центров зависит от надлежащего оснащения муниципальных органов власти, для пресечения угрозы применения террористами беспилотных авиационных систем (БАС) против «слабозащищенных целей» нужно наладить тесное взаимодействие между правительственными агентствами и поставщиками технических средств противодействия БАС.

Однако тот факт, что для различных типов уязвимых объектов могут потребоваться индивидуальная стратегия и законодательные решения, не делает менее важной задачу правительств по разработке всеобъемлющего подхода к их защите. Такой подход должен учитывать общие задачи первостепенной важности и проблемы, выявлять общие оперативные потребности и оптимизировать использование имеющихся ресурсов и инструментов для целей предотвращения, реагирования и восстановления.



Программный документ 1.

**Реагирование на террористические угрозы против «слабозащищенных целей» — аналитическая справка ИДКТК** (<https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-analytical-brief-soft-targets.pdf>)

Исполнительный директорат Контртеррористического комитета Организации Объединенных Наций (ИДКТК) подготовил указанную справку в соответствии с резолюцией 2395 (2017) Совета Безопасности Организации Объединенных Наций, в которой ИДКТК предписывается проводить аналитическую работу по возникающим проблемам, тенденциям и событиям и предоставлять свои аналитические наработки всей системе Организации Объединенных Наций. В ней подчеркивается также важность вовлечения гражданского общества в инициативы по защите «слабозащищенных целей» и особо отмечается необходимость расширения обмена информацией и укрепления доверия в целях повышения устойчивости без разглашения конфиденциальной информации или нарушения образа жизни населения.





Программный документ 2.

**Анталийский меморандум о защите «слабозащищенных целей» в контексте борьбы с терроризмом – Глобальный контртеррористический форум (ГКФ)** ([www.thegctf.org/About-us/GCTF-framework-documents](http://www.thegctf.org/About-us/GCTF-framework-documents))

Примеры передового опыта, приведенные в Меморандуме, является частью Инициативы ГКФ по защите «слабозащищенных целей», в рамках которой приводятся информация и указания для правительств и частного сектора в отношении их совместной работы по формированию политики, определению примеров практики, разработке руководящих принципов, программ и подходов в отношении защиты своих граждан от террористических нападений на «слабозащищенные цели». В Меморандуме признается, что ни один план или стратегия не в состоянии обеспечить защиту всех потенциальных целей, и в этой связи предпринимается попытка обобщить опыт, накопленный по этой теме в ходе различных региональных практикумов, проведенных в 2016 и 2017 годах.

Сформулированные 13 примеров передового опыта сгруппированы в три тематических блока:

1. понимание угрозы, выявление и определение приоритетности «слабозащищенных целей» на основе постоянной оценки рисков и налаженного эффективного обмена информацией, способствующего практическому сотрудничеству и взаимодействию на всех уровнях управления (международном, национальном, региональном и местном);
2. создание государственно-частных партнерств в интересах налаживания и совершенствования сотрудничества в области безопасности и вовлечение государственного сектора путем четкого и последовательного информирования о характере угрозы и надлежащих мерах обеспечения готовности;
3. подготовка, планирование и обеспечение защиты путем определения приоритетности ресурсов, задействования заинтересованных сторон, проведения учений и подготовки специалистов для повышения степени осведомленности правительства, соответствующих отраслей и общественности и степени готовности к предупреждению, реагированию и восстановлению.



Программный документ 3.

**Справочник по предупреждению терроризма и обеспечению готовности к нему – Международный центр по борьбе с терроризмом (МЦБТ)** (<https://icct.nl/handbook-of-terrorism-prevention-and-preparedness>)

Справочник, подготовленный Международным центром по борьбе с терроризмом (МЦБТ), является обширным ресурсом, который охватывает различные аспекты упреждающего противодействия терроризму, начиная от предупреждения радикализации и заканчивая предотвращением подготовительных актов и обеспечением готовности к смягчению последствий нападений.

Глава 27, в частности, посвящена теме «Эшелоны превентивных мер для защиты слабозащищенных целей от террористических нападений», в основе которой лежит идея о том, что хотя отдельные эшелоны могут быть недостаточными для предотвращения террористического нападения, их сочетание может стать мощным

превентивным инструментом. В Справочнике определены 13 «эшелонов превентивных мер» (ЭПМ) для защиты «слабозащищенных целей» на среднем и последующем уровнях<sup>26</sup>:

ЭПМ1: привлечение профессиональных мониторинговых агентств для сбора на постоянной основе информации из традиционных открытых источников (например, печатные средства массовой информации, радио, телевидение, научные исследования и сообщения неправительственных организаций);

ЭПМ2: отслеживание имеющей потенциальные насильственные последствия онлайн экстремистской деятельности, осуществляемой в социальных сетях, в «темном» и «глубоком интернете» (например, ненавистнические высказывания, которые могут являться признаком подготовки преступлений на почве ненависти, включая терроризм);

ЭПМ3: ведение сбора разведывательных данных путем наблюдения за известными и подозреваемыми экстремистами, экстремистскими группами и их спонсорами, а также прослушивания их разговоров (например, путем использования аппаратуры прослушивания для мониторинга их телефонов, компьютеров, автомобилей и домов);

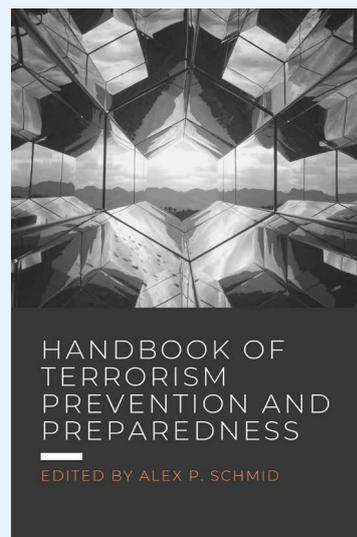
ЭПМ4: использование действующих под прикрытием агентов для внедрения в воинственно настроенные группы и/или вербовки информаторов из состава таких групп (например, террористов, которые выходят на свободу после отбытия срока наказания и вновь примыкают к своей группе), а также проведение допускаемых законом спецопераций;

ЭПМ5: обмен обработанной (не предварительной) разведывательной информацией (технической и агентурной) в пределах государственных учреждений и между ними, а также с пользующимися доверием службами разведки и безопасности за рубежом;

ЭПМ6: анализ террористической пропаганды и подготовка материалов для противодействия ей и альтернативных материалов, подкрепленных заслуживающими доверия действиями по предотвращению и пресечению (дальнейшей) радикализации;

ЭПМ7: проведение работы среди членов семей и друзей юношей и девушек, находящихся под воздействием радикальных идей, с целью побудить их конфиденциально сообщать о своих опасениях доверенной организации (не полиции или спецслужбам), предоставляя им гарантии того, что это не приведет к аресту членов их семей или друзей, а даст им возможность связаться с консультантами из программ наставничества молодежи или дерадикализации;

ЭПМ8: наблюдение за имеющими уголовное прошлое и/или проблемы с психическим здоровьем молодыми людьми, которые могут склоняться к тому, чтобы вступить в экстремистские группы, и подготовка специальных программ (например, в области спорта и профессионального обучения) в интересах таких молодых людей, относящихся к группе риска;



26 В то время как на среднем уровне деятельность по предотвращению нацелена на уменьшение риска подготовки террористической кампании той или иной террористической группой, на последующем уровне она направлена на смягчение риска осуществления отдельных террористических операций.

### Программный документ 3 (продолжение)

ЭПМ9: создание стимулов для разочаровавшихся членов террористических организаций, чтобы побудить их покинуть их группы и впоследствии, с их согласия, опубликовать их истории и помочь им найти род занятий;

ЭПМ10: выплата вознаграждения за полученную от общественности ориентировочную информацию, которая может помочь предотвратить террористическое нападение или привести к аресту воинствующих экстремистов и террористов;

ЭПМ11: мониторинг и отслеживание конкретных общеуголовных преступлений (таких как хищение взрывчатых веществ), которые могут совершаться в связи с подготовкой террористического нападения;

ЭПМ12: заблаговременная разработка протоколов быстрого реагирования на достоверные предупреждения о нападениях (например, в социальных сетях), полученные от исполнителя или представителя террористической организации;

ЭПМ13: публикация в средствах массовой информации или социальных сетях общественных предупреждений при получении достоверной новой информации о готовящемся террористическом нападении, а также рекомендаций населению проявлять бдительность и обращать внимание на установленных подозреваемых лиц и на подозрительные предметы и создание в этой связи специальной телефонной «горячей линии» для обращения к службам экстренного реагирования.

#### 4.1.2.1 Разработка стратегии в отношении «слабозащищенных целей»

В Мадридских руководящих принципах<sup>27</sup> государствам-членам предлагается в сотрудничестве с местными властями «разрабатывать, осуществлять и применять на практике такие стратегии и планы действий по снижению риска террористических нападений на важнейшие объекты инфраструктуры и «слабозащищенные цели», которые предусматривают объединение и эффективное использование возможностей соответствующих государственных и частных заинтересованных сторон». (Руководящий принцип 50-С)

Рекомендуется, чтобы стратегии, принимаемые на национальном уровне, являлись результатом широких консультаций между государственными ведомствами, организациями частного сектора/операторами объектов и организациями гражданского

общества (см. раздел 3.3.2) и имели целью решение ряда важнейших вопросов, таких как:

- что представляет собой «слабозащищенные цели» и какие критерии следует использовать для их определения?
- Как будет определяться и оцениваться спектр угроз в отношении «слабозащищенных целей»?
- В чем заключаются роли и обязанности отдельных государственных ведомств и различных уровней власти (например, федеральной, штата, округа, муниципального образования) в устранении угрозы и реагировании на инцидент?
- Какие органы власти и какие процедуры должны быть задействованы для управления рисками и регулирования кризисов?
- Какие формы государственно-частного партнерства могли бы быть полезны

<sup>27</sup> 27 и 28 июля 2015 года Контртеррористический комитет (КТК) Совета Безопасности Организации Объединенных Наций провел специальное заседание в Мадриде, Испания, чтобы обсудить последующие меры по осуществлению резолюции 2178 (2014) Совета Безопасности, касающейся наилучших способов сдерживания потока иностранных боевиков-террористов. На этом заседании присутствовали представители государств-членов, международных и региональных организаций, научных кругов и гражданского общества. Участники определили 35 руководящих принципов, которые впоследствии были одобрены Советом Безопасности (S/2015/939). 13 декабря 2018 года КТК провел специальное заседание, в ходе которого подготовил добавление к существующим руководящим принципам (S/2018/1177), дополнив их 17 новыми принципами.

(в том числе с операторами объектов), как будут определяться заинтересованные стороны из числа представителей частного сектора и какие каналы будут использоваться для поддержания эффективного обмена информацией меж-

ду государственным и частным секторами? (см. вставку 3)

- Каким образом предполагается вовлечь организации гражданского общества и широкую общественность в общие усилия по защите?



Вставка 3.

### Государственно-частные партнерства (ГЧП) для защиты «слабозащищенных целей»

В Мадридских руководящих принципах, в частности принципах 50 и 51, государствам-членам рекомендуется сформулировать свой подход к ГЧП для защиты «слабозащищенных целей» на основе следующих действий:

- создать или укрепить механизмы для обмена информацией, экспертными знаниями (включая инструментарий и руководящие указания) и опытом между государственными и частными заинтересованными сторонами в целях расследования террористических нападений на (слабозащищенные) цели и реагирования на них;
- внедрить процедуры для обмена информацией об оценке рисков между правительством, отраслевыми ведомствами и частным сектором в интересах содействия повышению осведомленности о положении дел и укрепления безопасности «слабозащищенных целей» и повышения их устойчивости к внешним воздействиям;
- внедрить процедуры для обмена соответствующей информацией с партнерами из отраслевых ведомств и частного сектора, например, путем предоставления допуска к засекреченной информации и повышения осведомленности;
- разработать механизмы сотрудничества, оказания поддержки владельцам предприятий и эксплуатирующим компаниям, а также управляющим объектами инфраструктуры и, в случае необходимости, обмена информацией о планах, политике и процедурах.

Таким образом, всеобъемлющая стратегия, охватывающая «слабозащищенные цели» в различных секторах и сферах деятельности, станет основой для разработки подстратегий или планов действий по защите конкретных типов уязвимых объектов. Кроме того, она должна быть совместима с параллельными правительственными стратегиями, которые могут быть приняты в таких смежных областях, как защита критически важных объектов инфраструктуры, борьба с терроризмом, обеспечение национальной безопасно-

сти и регулирование кризисов. Разработка национальной стратегии в отношении «слабозащищенных целей» может даже обеспечить возможность для пересмотра всего пакета взаимосвязанных стратегий и планов действий с целью обеспечения оперативной последовательности, координации действий между многочисленными заинтересованными сторонами, рационализации процедур и оптимизации использования ресурсов.



### Конкретный пример 1. **Стратегия защиты мест скопления людей от терроризма, принятая в Австралии**

Принятая в Австралии Стратегия защиты мест скопления людей от терроризма опирается на создание прочных и надежных партнерских отношений между всеми уровнями власти и структурами, которые несут ответственность за места скопления людей (владельцами и операторами). Ее цель заключается в том, чтобы сделать места скопления людей как можно более устойчивыми к террористическим атакам, сохранив при этом возможность доступа к этим местам и пользования ими.

Эта стратегия была принята в 2017 году и включает четыре основных элемента: 1) создание более прочных партнерств; 2) обеспечение более эффективного обмена информацией и руководства; 3) обеспечение эффективной охраны и безопасности; и 4) повышение устойчивости.

*Источник: ANZCTC, 2017.*



### Конкретный пример 2. **Обзор плана обеспечения безопасности «слабозащищенных целей» и мест скопления людей –Министерство внутренней безопасности Соединенных Штатов**

Обзор указанного плана позволяет получить представление о подходе, который применяет Министерство внутренней безопасности Соединенных Штатов (МВБ) для координации своей деятельности по усилению безопасности и устойчивости «слабозащищенных целей» и мест скопления людей (СЦ-МСЛ) на всей территории Соединенных Штатов.

Управление рисками и регулирование кризисов осуществляется на основе следующих принципов:

- единство цели, которая охватывает широкую общественность, владельцев и операторов СЦ-МСЛ, партнеров из сектора безопасности, партнеров из числа властей штатов, местных, племенных и территориальных властей, а также федеральное правительство;

функции МВБ по обеспечению безопасности тех мест, за которые оно несет ответственность, и по оказанию поддержки другим заинтересованным сторонам в выполнении их обязанностей по обеспечению безопасности СЦ-МСЛ осуществляются по четырем направлениям: 1) проведение непосредственных операций по обеспечению безопасности некоторых объектов и мест, которые могут считаться СЦ-МСЛ, включая транспортную инфраструктуру, порты, водные пути и т.д.; 2) обеспечение осведомленности, обмен разведывательными данными и информацией; 3) наращивание потенциала и возможностей партнеров; 4) проведение научно-исследовательских и опытно-конструкторских работ.

МВБ осуществляет ряд инициатив, в том числе в следующих областях:

- повышение степени осведомленности путем проведения масштабной кампании по образованию и распространению информации;
- взаимодействие с ключевыми международными партнерами для обмена передовым опытом и информацией об извлеченных уроках;
- повышение степени осведомленности о ресурсах МВБ, имеющих отношение к СЦ-МСЛ, и доступе к ним путем разработки справочников, руководств и инструментов для самостоятельного изучения;
- фокусирование и стимулирование инвестиций в безопасность СЦ-МСЛ путем привлечения субсидий и технической помощи для усиления безопасности СЦ-МСЛ и стимулирования инвестиций на местах;
- содействие проведению целенаправленных научно-исследовательских и опытно-конструкторских работ по вопросам безопасности СЦ-МСЛ.

*Источник: Министерство внутренней безопасности Соединенных Штатов, 2018 год.*





Программный документ 4.

**Справочник по вопросам создания государственно-частных партнерств для защиты уязвимых целей – ЮНИКРИ, 2010 год**  
([https://unicri.it/topics/public\\_private\\_security\\_policies](https://unicri.it/topics/public_private_security_policies))

ЮНИКРИ разработал указанный справочник по итогам серии практикумов, совещаний экспертов, аналитических исследований, имеющих практическую направленность, и тестовых мероприятий. Он предназначен для практических специалистов по безопасности из государственных структур и частных компаний и содержит построенную на основе продуманной и прагматичной концепции методологию, состоящую из десяти шагов, а также несколько инструментов, которые могут быть использованы для создания или укрепления ГЧП в целях предотвращения угроз безопасности на национальном и/или местном уровнях и реагирования на них.

Он дополняет, а не подменяет существующие национальные или региональные планы или структуры, призванные обеспечивать защиту уязвимых «слабозащищенных целей».



Программный документ 5.

**Анталийский меморандум: создание государственно-частных партнерств – ГКФ, 2017 год** ([www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth GCTF Coordinating Committee Meeting/GCTF - Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context.pdf?ver=2017-09-17-010844-720](http://www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth%20GCTF%20Coordinating%20Committee%20Meeting/GCTF%20Antalya%20Memorandum%20on%20the%20Protection%20of%20Soft%20Targets%20in%20a%20Counterterrorism%20Context.pdf?ver=2017-09-17-010844-720))

В Меморандуме содержится целый раздел, посвященный описанию примеров передовой практики в области вовлечения отраслевых структур посредством «четкого и последовательного информирования о характере угрозы и надлежащей готовности». К ним относятся следующие:

пример передовой практики № 6: вовлечение всех заинтересованных сторон в процесс создания эффективной национальной антитеррористической структуры, предусматривающей распределение обязанностей по обеспечению готовности «слабозащищенных целей» – профилактика, защита, смягчение последствий, реагирование, восстановление;

пример передовой практики № 7: укрепление сотрудничества на всех уровнях власти и сотрудничества между правительством и частным сектором, а также расширение обмена информацией и опытом между государствами;

пример передовой практики № 8: установление доверительных отношений между государственными и частными структурами безопасности и обеспечение более активного участия отраслевых структур в усилиях по обеспечению безопасности;

пример передовой практики № 9: привлечение граждан и работников частного сектора к участию в обеспечении безопасности путем сообщения о подозрительной деятельности.

#### 4.1.2.2 Определение «слабозащищенной цели»

В своей резолюции 75/291 Генеральная Ассамблея призывает государства-члены активизировать усилия по укреплению безопасности и защиты особо уязвимых целей, включая религиозные объекты, образовательные учреждения, туристические объекты, городские центры, культурные и спортивные мероприятия, транспортные узлы, митинги, шествия и автоколонны, а также повышению выносливости к террористическим нападениям, в частности в области гражданской защиты...». В Мадридских руководящих принципах к государствам-членам обращен призыв «определять на основе постоянного анализа возможностей, намерений и прошлых нападений террористов, какие объекты следует считать (...) «слабозащищенными целями» в национальном контексте». (Принцип 50-B)

Хотя теоретически объектом нападения может стать любое пространство, ограниченный объем ресурсов для целей обеспечения безопасности заставляет придерживаться прагматичного подхода, основанного на определении приоритетности целей. Заблаговременное выявление объектов, подверженных наибольшему риску, имеет основополагающее значение для принятия обоснованных и подкрепленных разведывательной информацией решений о том, на какие цели, в каком объеме и когда следует выделять ресурсы для проведения профилактических, правоохранительных и антикризисных мероприятий. Понимание динамики террористической угрозы, намерений и потенциала субъектов, создающих такую угрозу на территории государств-членов, также имеет существенно важное значение для выявления новых или приоритетных «слабозащищенных целей».

Как отмечается в Анталийском меморандуме ГКФ, «слабозащищенные цели не имеют конкретного характера и потенциально могут представлять собой любое место, где скапливается или собирается

большое количество людей. По этой причине концепция охраны должна иметь динамичный и целевой характер и ориентироваться на географические районы, не допуская статичности в той или иной мере и заикленности на конкретных объектах». (Источник: ГКФ, 2017 год, пример передовой практики № 4)

Кроме того, в то время как большинство критически важных объектов инфраструктуры остаются уязвимыми на постоянной основе, поскольку от операторов ожидается бесперебойное предоставление основных услуг, объекты, которые обычно определяются как «слабозащищенные цели», часто становятся уязвимыми только в определенные периоды времени (например, во время конкретных событий, таких как концерт или открытие уличного рынка в определенные дни недели)<sup>28</sup>. Поэтому фактические уровни защиты не обязательно должны сохраняться неизменными в течение времени, а скорее должны адаптироваться к конкретным условиям использования объектов<sup>29</sup>.

Плотность скопления людей, безусловно, является одним из основных критериев для определения целесообразности квалификации того или иного места в качестве «слабозащищенного» для целей применения усиленных мер безопасности. Вместе с тем наличие большого скопления людей не может являться единственным критерием при оценке необходимости и уровня особой охраны конкретного объекта. Необходимо учитывать и другие критерии, в частности особую привлекательность того или иного объекта или события для террористов, например, вследствие его символического значения. Другим важным фактором является результат национального или местного анализа угроз, который определяет те или иные объекты как цель потенциального нападения.

Поскольку ключом к определению соответствующих объектов в качестве «слабозащищенных целей» является оценка местных условий и сценариев угроз, местные заинтересованные стороны, включая

28 Как отмечалось в разделе 1.2, обоснования для защиты «слабозащищенных целей» и критически важных объектов инфраструктуры являются различными, в связи с чем критерии, применяемые для квалификации тех или иных объектов инфраструктуры в качестве критически важных (а именно, степень ущерба, который нападение на них нанесет экономике, окружающей среде и т. д.), могут не подходить для идентификации «слабозащищенных целей».

29 Некоторые объекты, например, могут неожиданно стать уязвимыми, в частности когда государственные органы получают уведомление о том, что в определенном месте и в определенную дату будет проведена демонстрация.

операторов объектов и местные власти, становятся ключевыми участниками процесса определения приоритетности на основе своего досконального владения ситуацией и наличия прямого доступа к информации о местной динамике, людских потоках, времени проведения мероприятий и т. д.

#### 4.1.2.3 Создание организационной и оперативной структуры для управления рисками и регулирования кризисов

В резолюции 2396 (2017) Совета Безопасности Организации Объединенных Наций подчеркивается, что государствам-членам необходимо подготовить национальные оценки рисков и угроз, провести их обзор или внести в них изменения таким образом, чтобы в них принимались во внимание «слабозащищенные цели», и разработать соответствующие планы на случай угрозы террористических нападений и планы чрезвычайного реагирования в случае таких нападений.

Эта рекомендация получила дальнейшее развитие в Мадридских руководящих принципах, в которых к государствам-членам обращен призыв разработать меры по защите «слабозащищенных целей» путем «регулярного проведения оценки рисков с учетом меняющегося характера угрозы и противника, в том числе с использованием существующих инструментов и руководящих указаний, разработанных международными и региональными организациями». (Принцип 50 b)

Руководствуясь принципом 51, что в своих дальнейших усилиях по защите критически важных объектов инфраструктуры и «слабозащищенных целей» от террористических нападений государствам-членам, действующим в сотрудничестве с местными органами власти, следует также, среди прочего, рассмотреть возможность:

a) обновления планов действий в чрезвычайной обстановке, включая руководящие указания, планы проведения учений и подготовки сотрудников правоохранительных органов, других соответствующих министерств и отраслевых ведомств, с тем чтобы обеспечить учет реально существующих угроз, усовершенствовать стратегии и обеспечить адаптацию заинтере-

сованных сторон к изменяющимся угрозам;

- b) создания национальных структур и механизмов в поддержку принятия решений с учетом фактора риска, обмена информацией и государственно-частного партнерства как для правительства, так и для отраслевых ведомств, в том числе в целях налаживания совместной работы по определению приоритетов, и совместной разработки соответствующих материалов и инструментов, таких как общие руководящие принципы наблюдения или конкретные меры, предлагаемые для защиты объектов различных типов (например, стадионов, гостиниц, торговых центров или школ);
- c) внедрения процедур для обмена информацией об оценке рисков между правительством, отраслевыми ведомствами и частным сектором в интересах содействия повышению осведомленности о положении дел и укрепления безопасности «слабозащищенных целей» и повышения их устойчивости к внешним воздействиям;
- d) внедрения процедур для обмена соответствующей информацией с партнерами из отраслевых ведомств и частного сектора, например, путем предоставления допуска к засекреченной информации и повышения осведомленности.

Для любой национальной стратегии, касающейся уязвимых «слабозащищенных целей», важно, чтобы структура управления рисками и регулирования кризисов обеспечивала задействование различных заинтересованных сторон и предусматривала опору на результаты оценки угроз, проведенной на уровне руководства (как на национальном, так и на местном), на отраслевом уровне (например, анализ угроз, затрагивающих конкретные объекты, такие как религиозные учреждения, образовательные центры, туристические объекты, городские центры) и на уровне операторов отдельных объектов. Учитывая тесный контакт организаций гражданского общества с местным населением и/или их специальные знания по вопросам безопасности, крайне важно привлечь их на ранней стадии планирования национальной стратегии.



### Конкретный пример 3. План «Вижипират», принятый во Франции

Принятый во Франции план «Вижипират» обеспечивает организационную и оперативную основу для управления рисками и регулирования кризисов в связи с защитой «слабозащищенных целей» от терроризма. В реализации этого плана участвуют государство, местные органы власти, предприниматели и граждане. Совершенные в стране в 2015 и 2016 годах террористические нападения на несколько «слабозащищенных целей» потребовали пересмотра плана «Вижипират», чтобы адаптировать его к ситуациям, в которых существует особо высокий уровень угрозы. Текущая версия плана предусматривает три основных компонента:

1. формирование охватывающей все гражданское общество культуры индивидуального и коллективного подхода к вопросам безопасности;
2. определение трех уровней безопасности на основе оценки угрозы и размещение в местах общественного пользования хорошо заметных информационных знаков, а именно:
  - a) *уровень повышенной бдительности*: соответствует обычному протоколу безопасности и предусматривает осуществление 100 различных мер;
  - b) *повышенный уровень безопасности – наличие риска нападения*: государство принимает меры реагирования на высокую или даже очень высокую террористическую угрозу. В дополнение к обычным мерам безопасности может быть задействовано несколько специальных мер;
  - c) *уровень чрезвычайной ситуации при нападении*: может быть введен сразу после нападения или при появлении угрозы со стороны известной нелокализованной террористической группы. Этот уровень устанавливается на ограниченное время, необходимое для проведения операций по регулированию кризисов. Он позволяет мобилизовать исключительные ресурсы;



### Конкретный пример 3. (продолжение)

#### 3. принятие новых мер для усиления государственного противодействия терроризму.

На практике анализ угроз, проводимый компетентными спецслужбами, используется Генеральным управлением по обороне и национальной безопасности (ГУОНБ)<sup>30</sup> в качестве основы для выработки общей позиции в вопросах обеспечения безопасности в рамках плана «Вижипират». Такая позиция также предусматривает принятие мер:

- по случаю крупных национальных мероприятий (например, спортивных соревнований, международных саммитов);
- по случаю определенных ключевых дат (например, начало учебного года, празднование окончания года);
- в случае совершения нападения во Франции или за рубежом, чтобы срочно адаптировать национальную систему защиты.

В целом, план «Вижипират» включает около 300 мер, в том числе постоянные меры, применяемые в отношении 13 основных сфер деятельности (транспорт, здравоохранение и т. д.), и дополнительные меры, задействуемые в зависимости от характера и уровня оценки террористической угрозы. Некоторые из этих мер засекречены. План «Вижипират» распространяется на определенные области благодаря применению средств, предусмотренных специальными планами действий (планы ХБРЯ, «Пиратейр-Интрусейр», «Пиратейр-мер», «Пиранет», «Метропират», расширенный план «Перехват»).

Источник: <https://www.gouvernement.fr/risques/comprendre-le-plan-vigipirate>.



<sup>30</sup> ГУОНБ находится в подчинении премьер-министра Франции и является межведомственным органом, который оказывает содействие главе правительства в разработке и реализации стратегий обеспечения безопасности и обороны.



#### Конкретный пример 4.

### Национальная система идентификации рисков, принятая Шведским гражданским агентством по чрезвычайным ситуациям

В ответ на просьбу правительства Швеции провести национальную оценку рисков Шведское гражданское агентство по чрезвычайным ситуациям подготовило доклад, основанный на выборке рисков, определенных государственными органами и местными административными советами. Эти риски охватывают широкий спектр инцидентов, включая, в частности, терроризм и риск кибератак.

В докладе представлены также несколько типичных случаев, которые могут стать для Швеции поводом для обращения за международной помощью. В приложениях приводятся сценарии из прошлого, по которым была проведена оценка с помощью различных методов.

Источник: National Risk Identification Report, 2011.

#### 4.1.2.4 Внедрение коммуникационной стратегии

Важно обеспечивать применение коммуникационных стратегий<sup>31</sup> на всех этапах процесса управления рисками и регулирования кризисов, при чем все государственные ведомства должны согласовать факты и подход, которого следует придерживаться. Коммуникационные планы должны предусматривать не только информирование и повышение степени осведомленности различных категорий заинтересованных сторон на разных этапах цикла деятельности по обеспечению безопасности и в случае возникновения кризиса, но и содействовать сохранению социальной сплоченности и недопущению стигматизации определенных сообществ или их членов.

Одним из основополагающих аспектов любой коммуникационной стратегии является определение каналов и способов

охвата широкой общественности. В этой связи в Анталийском меморандуме ГКФ определены следующие примеры передовой практики, которыми правительства должны руководствоваться до, во время и после нападения на «слабозащищенные цели» (ГКФ, 2017 год, пример передовой практики № 13):

**до нападения:** распространять информацию о реалистичных оценках риска, чтобы управлять ожиданиями общественности. Цель заключается в том, чтобы максимально повысить пользу от оповещений и не позволить террористам управлять восприятием угрозы. Задача состоит в том, чтобы просвещать население и предлагать полезные советы, избегая непреднамеренного повторения заявлений террористов, не перегружая население постоянным потоком информации и не вызывая усталости от угроз<sup>32</sup>;

**во время нападения:** определять наилучшие способы реагирования и информа-

31 Контртеррористический центр Организации Объединенных Наций КТУ ООН играет ведущую роль в осуществлении проекта «Предотвращение насильственного экстремизма посредством стратегических коммуникаций», который может представлять интерес и принести пользу в настоящем контексте. URL: <https://www.un.org/counterterrorism/cct/strategic-communication>.

32 Что касается деятельности по предотвращению, то в Анталийском меморандуме ГКФ особо отмечаются также шаги, которые правительства могут предпринять в плане коммуникации, чтобы повысить склонность и способность населения выявлять угрожающую активность. В примере передовой практики № 9 указывается, что «предостерегающие надписи, рекламные щиты и объявления в общественном транспорте или в местах общественного пользования могут повысить степень осведомленности общественности, а кампании по информированию общественности могут принести пользу, если они правильно сфокусированы. Следует транслировать объявления службы общественной информации по радио и телевидению. Для стран, в которых отсутствует план информирования общественности, хорошей отправной точкой являются регулярные или личные встречи с представителями торговых организаций или владельцами и операторами объектов, вызывающих обеспокоенность общественности».

цию, которую следует обнародовать. Та часть принятого правительством плана реагирования, которая касается информирования общественности, имеет столь же важное значение, как и оперативные меры. Следует предоставить населению четкие инструкции относительно того, какие места следует избегать, какими убежищами можно воспользоваться, и другую практическую информацию. Как отмечалось выше, информация должна носить сбалансированный характер, чтобы она не стала непреднамеренным отголоском заявлений террористов;

после нападения: как можно быстрее вернуться к нормальной жизни. Следует подготовиться к действиям в социальных сетях и до нападения подготовить сообщения, чтобы транслировать их после его совершения. Кроме того, крайне важно получить доступ к коммуникационным планам сразу же после нападения, чтобы зафиксировать извлеченные уроки.

### 4.1.3 Правоприменительная деятельность

Ключевые роли и обязанности правоохранительных органов по защите «слабозащищенных целей» делятся на следующие три основные категории:

1. *поддержка операторов уязвимых объектов*: виды поддержки, которую могут обеспечить правоохранительные органы, включают от подготовки оценок угроз/факторов уязвимости и разработки планов действий в чрезвычайных ситуациях до оказания помощи в организации учений и подготовки персонала объекта и службы охраны, а также помощи в определении возможностей привлечения средств для модернизации систем безопасности. Установление доверительных отношений с операторами уязвимых объектов побудит последних принять инициативный подход в сфере сотрудничества в вопросах безопасности, что будет способствовать повышению степени осведом-

ленности и готовности правоохранительных органов;

2. *расследование террористических нападений на уязвимые цели или деятельности по подготовке к их совершению*: правоохранительные органы должны расширять проводимые ими расследования деятельности более широких сетей, стоящих за нападением или подготовкой к его совершению. В свою очередь, успех этих расследований зависит от активной поддержки со стороны соответствующих разведывательных служб, которые могут установить вероятность нападения и предоставить информацию о передвижениях лиц, находящихся под наблюдением. Кроме того, сотрудники органов уголовного правосудия должны быть знакомы с такими процессами международного сотрудничества, как оказание правовой взаимопомощи, обмен правоохранительной информацией, выдача, а также обработка и сохранение доказательств и обмен ими для использования в уголовных процессах<sup>33</sup>.

3. *работа с населением*: в Анталийском меморандуме описывается опыт нескольких заинтересованных сторон и отмечается, что в качестве «превентивной меры, направленной на выявление и решение проблем до их эскалации» важно использовать сотрудников полиции для налаживания взаимодействия с населением, разъяснения законов и оказания людям помощи в понимании их прав и обязанностей. (ГКФ, 2017 год, пример передовой практики № 9) Работа с населением является важным аспектом деятельности по охране общественного порядка, составляющей часть более широкой правоохранительной стратегии, в которой делается упор на партнерские, совместные усилия полиции и местного населения.

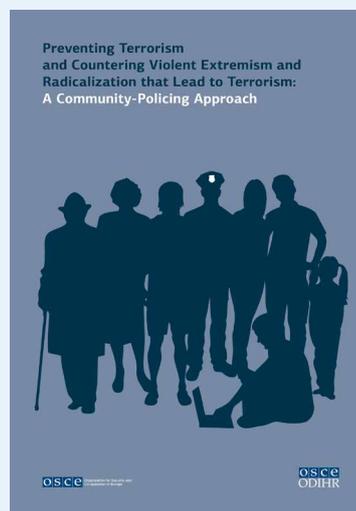
<sup>33</sup> В той мере, в которой нападения на уязвимые цели имеют существенные транснациональные аспекты, например, когда жертвами являются граждане нескольких разных стран, органы уголовного правосудия пострадавших стран могут рассмотреть возможность применения таких механизмов, как передача уголовного производства, что позволит сосредоточить разбирательство в рамках одной юрисдикции.



Программный документ 6

**Предупреждение терроризма и борьба с насильственным экстремизмом и радикализацией, ведущими к терроризму: подход, основанный на взаимодействии полиции с населением – Организация по безопасности и сотрудничеству в Европе (ОБСЕ), 2014 год**  
([www.osce.org/files/f/documents/1/d/111438.pdf](http://www.osce.org/files/f/documents/1/d/111438.pdf))

Это руководство затрагивает в совокупности три важных приоритетных тематических направления в работе ОБСЕ, которые недавно были подтверждены государствами-участниками. Как указано в Консолидированной концептуальной базе ОБСЕ для борьбы с терроризмом, принятой в декабре 2012 года, двумя стратегическими направлениями контртеррористической деятельности ОБСЕ являются «основанное на комплексном подходе противодействие насильственному экстремизму и радикализации, ведущим к терроризму (НЭРВТ)» и «продвижение и защита прав человека и основных свобод в контексте контртеррористических мер». «Содействие развитию партнерских отношений между полицией и населением/взаимодействия полиции с местным населением» является еще одним приоритетным тематическим направлением, обозначенным в Стратегической концепции ОБСЕ в отношении деятельности, связанной с полицейскими функциями (принята в июле 2012 года).



Указанное руководство содержит рекомендации по основным вопросам, от решения которых может зависеть успех или неудача усилий полиции по использованию подхода на основе сотрудничества с местным населением в целях предупреждения терроризма и противодействия НЭРВТ. Таким образом, это руководство предназначено в первую очередь для разработчиков политики и руководства полицейских органов. Вместе с тем оно также может быть полезным для представителей гражданского общества, занимающихся этими вопросами, и, прежде всего, для общественных лидеров. Оно может послужить в качестве общего справочного документа для содействия развитию взаимопонимания и доверия, а также при налаживании диалога между полицией и общественностью по вопросам, касающимся угрозы терроризма и НЭРВТ. Содержащиеся в нем разделы охватывают следующие аспекты:

- ключевые концепции, связанные с предупреждением терроризма и ориентированными на взаимодействие с населением подходами к контртеррористической деятельности;
- оценка эффективности взаимодействия полиции с населением с точки зрения усилий по предупреждению терроризма и противодействию НЭРВТ;
- рекомендации по вопросам обеспечения учета прав человека и стандартов гендерного равенства в процессе взаимодействия полиции с населением;
- практические рекомендации по таким конкретным вопросам осуществления деятельности, как координация работы, постановка задач, обучение, коммуникация, обмен информацией, работа с конкретными группами и оценка результатов.

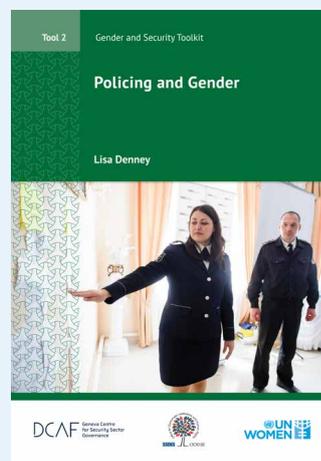
Руководство основано на анализе соответствующего опыта, накопленного рядом государств – участников ОБСЕ и партнерами ОБСЕ по сотрудничеству, а также на предыдущих публикациях ОБСЕ.



Программный документ 7.

**Полиция и гендерный фактор — Женевский центр по управлению сектором безопасности, Бюро ОБСЕ по демократическим институтам и правам человека, Структура «ООН-женщины», 2019 год**  
([www.osce.org/files/f/documents/e/9/442519.pdf](http://www.osce.org/files/f/documents/e/9/442519.pdf))

Публикация «Полиция и гендерный фактор» является частью серии пособий по теме «Гендерный фактор и безопасность», которая включает девять пособий и серию аналитических записок. Основная идея заключается в том, что «достижение гендерного паритета в рядах полиции и по линии полицейской деятельности — это не просто увеличение числа женщин. Задача заключается в преобразовании тех соотношений прав и возможностей, которые поддерживают неравенство и гендерное насилие. Задача заключается в обеспечении защиты прав человека всех людей и создании условий для их полноценного участия в общественной жизни. Предполагается, что полицейские службы обеспечивают учет гендерного фактора в силу международных и внутренних правовых обязательств, однако это необходимо и для повышения эффективности работы полиции, усиления безопасности общества и укрепления верховенства закона».



В указанном пособии изложен ряд вариантов обеспечения учета гендерного фактора и укрепления гендерного паритета в рядах полиции и по линии полицейской деятельности на основе опыта, накопленного в различных контекстах. В нем приведены рекомендации в виде примеров, контрольных списков и описания передовой практики.

#### 4.1.4 Сотрудники служб экстренного реагирования

Оперативность и эффективность действий сотрудников служб экстренного реагирования в случае террористического нападения играет ключевую роль в смягчении последствий кризиса и организации процесса восстановления<sup>34</sup>. Для этого важно, чтобы все, кто участвует в принятии мер реагирования на нападения на «слабозащищенные цели» (пожарные, полиция, службы экстренного реагирования и медицинские службы):

1. были обеспечены совместимыми средствами связи<sup>35</sup>;
2. заблаговременно до инцидента связывались с операторами объекта, чтобы

ознакомиться с его характеристиками в целях повышения оперативности и эффективности оказания экстренной помощи, если и когда она потребуется;

3. привлекали операторов объектов к участию в учениях и имитационных учениях в целях обеспечения готовности на случай, если потребуется задействовать экстренные процедуры (например, провести эвакуацию объекта);
4. рассмотрели возможность назначения контактного лица/координатора и обеспечили, чтобы операторы объекта знали, к кому и/или в какое ведомство следует обращаться для решения вопросов, связанных с принятием мер безопасности, включая обеспечение готовности и охраны.

<sup>34</sup> В то же время, крайне важно, чтобы службы экстренного реагирования планировали и выполняли свою работу с учетом того, что они сами могут стать объектом террористического насилия в результате вторичного нападения, когда они оказывают помощь жертвам террористического инцидента. Это требует последовательного анализа динамики угрозы со стороны террористических субъектов.

<sup>35</sup> В Мадридских руководящих принципах к государствам-членам обращен призыв «содействовать повышению эффективности взаимодействия в области обеспечения безопасности и управления кризисными ситуациями» (Принцип 50-Е).



#### Вставка 4. Расширенное понятие «оперативной совместимости»

Традиционно под оперативной совместимостью понимают техническую способность систем связи обеспечивать сопряженность/взаимодействие друг с другом. Однако в последнее время все большее распространение получает расширенное понятие оперативной совместимости, согласно которому принцип сопряженности должен предусматривать также взаимодействие групп специалистов, синхронизацию процедур и обеспечение обмена информацией, для чего предлагается, в частности, принять следующие меры:

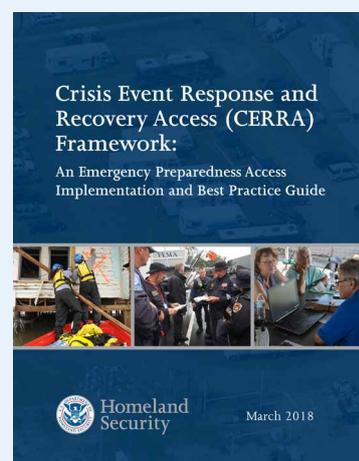
- принять нетехнические решения: обеспечить совместимость в работе специалистов и совместимость процедур; сформировать культуру оперативной совместимости;
- принять заблаговременные меры: назначить агентство или подразделение, единственная задача которого будет заключаться в обеспечении оперативной совместимости и интеграции; разработать простые практические решения;
- проявлять предусмотрительность: убедиться в том, что новые ИТ-системы, программы обучения персонала и сами сотрудники нацелены на обеспечение оперативной совместимости; убедиться в том, что поставщики способны выполнить свои обещания;
- обеспечить готовность: проводить учения, направленные исключительно на обеспечение интеграции критически важных функций между ведомствами;
- обеспечить максимально критический подход: составлять отчеты о результатах всех учений и обо всех инцидентах; составлять планы улучшения показателей с учетом местных реалий; не выходить за рамки разумных ожиданий;
- сделать оперативную совместимость задачей первостепенной важности в сфере общественной безопасности: если обеспечить защиту сотрудников служб экстренного реагирования, то они будут лучше подготовлены к защите населения, которому они служат.

*Источник:* выступление д-ра Донелла Харвина, Джорджтаунский университет, на организованном КТУ ООН совещании Группы экспертов по защите городских центров и туристических объектов, 15–16 июня 2021 года.



#### Программный документ 8. Рамочный план реагирования на кризисные события и посткризисного восстановления – Министерство вну- тренней безопасности Соединенных Штатов, 2018 год ([www.cisa.gov/publication/ crisis-event-response-and-recovery-access](http://www.cisa.gov/publication/crisis-event-response-and-recovery-access))

Этот рамочный план содержит адресованные компетентным ведомствам рекомендации по вопросам безопасного, надежного и эффективного контроля и координации доступа ключевых аварийно-восстановительных служб к пострадавшим районам во время чрезвычайных ситуаций. В нем изложены механизмы, инструменты, процессы и подходы для координации, утверждения и обеспечения доступа во время операций по реагированию и восстановлению.



### 4.1.5 Разведывательные службы

В рамках своего мандата по обеспечению национальной безопасности разведывательные службы являются крайне важными участниками деятельности по сбору и анализу информации о сделках, разговорах, перемещениях людей и товаров, которые могут свидетельствовать о подготовке террористических актов против уязвимых целей. Кроме того, они играют важную роль в анализе динамики исходящей от террористов угрозы в том, что касается их намерений и возможностей в плане совершения нападений. Их работа всегда должна вестись в соответствии с требованиями верховенства закона и с соблюдением международных обязательств в области прав человека<sup>36</sup> и гендерного равенства. В частности, все виды деятельности по наблюдению должны полностью соответствовать международным обязательствам, касающимся права на неприкосновенность частной жизни, и предусматривать эффективный и независимый механизм надзора. Роли и обязанности разведывательных служб включают следующее:

- оценка на постоянной основе общего характера и уровня угрозы, в том числе путем мониторинга социальных платформ и обработки поступающей от неправительственных субъектов информации для выявления признаков склонности отдельных лиц к насильственному поведению. Эта задача часто является сложной, особенно когда речь идет о лицах, которые в течение короткого периода времени самостоятельно проникаются радикальными идеями и формально не принадлежат ни к какой террористической организации;
- внедрение в террористические группы и используемые ими социальные платформы с целью получения информации о структуре, намерениях, ресурсах и возможностях, текущих планах по нанесению ударов по уязвимым объектам и т. д.<sup>37</sup>;
- сбор информации из открытых источников. Ценная информация не обязательно должна быть секретной или закрытой, поскольку террористические группы часто определяют цели и предоставляют оперативные указания о методах совершения нападений в общедоступных публикациях;
- налаживание или укрепление сотрудничества с правоохранительными органами, особенно на местном уровне, и с теми, кто занимается охраной общественного порядка, учитывая их близость к местным жителям, тесные контакты с ними и знание местных условий;
- сбор информации из различных/разнообразных источников и прогнозирование закономерностей (например, информация о хищении взрывчатых веществ в сопоставлении с информацией о выезде определенных субъектов из некоторых пунктов или их поездках в некоторые пункты). Из мелких деталей может складываться общая картина. Сами по себе такие детали не содержат никаких указаний на преступное поведение или намерения, однако в совокупности с другими имеющимися данными они могут способствовать выявлению опасных закономерностей;
- изучение возможности рассекречивания и/или цензурирования конфиденциальной информации, имеющей отношение к угрозам, чтобы ею можно было поделиться с другими государственными ведомствами и операторами уязви-

36 В 2010 году по просьбе Совета по правам человека Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартин Шейнин подготовил «Подборку оптимальных практических методов, применяемых в отношении законодательной и институциональной основы, и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью». Эта подборка была подготовлена по итогам процесса консультаций с участием представителей правительств, экспертов и практических специалистов. В целом, в ней приведено 35 примеров передовой практики. См. A/HRC/14/46, URL: <https://undocs.org/ru/A/HRC/14/46>.

37 Исполнители террористических нападений часто заранее размещают на социальных платформах сообщения о своем намерении нанести удар. В то же время, по мере повышения эффективности компаний, управляющих основными социальными сетями, в плане контроля за размещаемыми на их платформах сообщениями обмена террористическими сообщениями переходят на нишевые или специально разработанные социальные платформы, которые сложнее контролировать.

мых объектов в целях управления рисками<sup>38</sup>;

- учет гендерного фактора при планировании, сборе, анализе и распространении разведывательной информации в качестве способа поддержки выявления незамеченных признаков нестабильности, преодоления предубеждений, обеспе-

чения всестороннего понимания социального контекста и динамики, а также прогнозирования и смягчения потенциальных негативных последствий сбора и распространения разведывательной информации для гражданских и политических прав, а также прав человека соответствующих лиц.

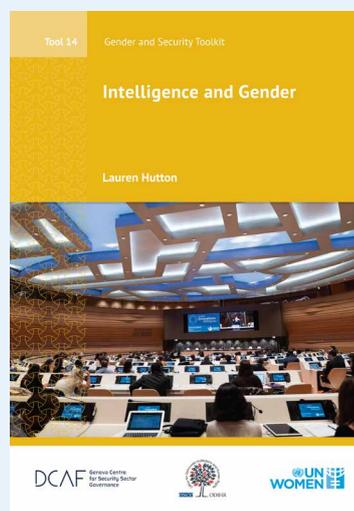


Программный документ 9.

**Разведка и гендерный фактор – Женевский центр по управлению сектором безопасности, Бюро ОБСЕ по демократическим институтам и правам человека, Структура «ООН-женщины», 2019 год**  
([www.osce.org/files/f/documents/f/2/447061.pdf](http://www.osce.org/files/f/documents/f/2/447061.pdf))

Публикация «Разведка и гендерный фактор» является частью серии пособий по теме «Гендерный фактор и безопасность», которая включает девять пособий и серию аналитических записок. Это пособие, в частности, содержит подборку примеров передовой практики, которые следует учитывать при разработке стратегий и процедур и/или проведении реформы разведывательного сообщества в целях содействия обеспечению гендерного паритета и учету гендерного фактора.

В основе указанного пособия лежит обеспокоенность тем, что «в свете закрытого и секретного характера разведывательных органов, потребовалось в целом больше времени для того, чтобы распространить инициативы по обеспечению учета гендерного фактора, реализуемые во всем государственном секторе и секторе безопасности, на разведывательное сообщество. Работа по реформированию разведывательных органов редко охватывает гендерные аспекты. Усилия по устранению гендерных диспропорций в разведывательных службах предприняты относительно недавно и определяются представлениями общества в целом о гендерных ролях, прогрессом в достижении гендерного равенства и уровнем демократизации».



## 4.2 Неправительственные субъекты

Что касается защиты уязвимых объектов, то Генеральная Ассамблея Организации Объединенных Наций прямо призвала «государства-члены установить или укреплять, сообразно обстоятельствам, национальные, региональные и международные партнерские отношения с заинтересованными сторонами, как государственными, так и частными, для обмена информацией и опытом в целях предотвращения террористических нападений, защиты от них, уменьшения их последствий, их расследования, реагирования на них и восстановления после таких нападений...»(п.73). Этим государства-члены признали важность создания многосторонних партнерств в целях предотвращения угрозы в отношении уязвимых целей и противодействия ей. В настоящем разделе рассматривается вопрос о том, как соответствующие заинтересованные стороны могли бы поддержать усилия правительств в этом направлении.

### 4.2.1 Операторы объектов

В зависимости от характера рассматриваемого объекта и применимой нормативно-правовой базы операторами уязвимых объектов могут быть структуры частного сектора, органы государственной власти или смешанные государственно-частные консорциумы. Хотя на разные категории заинтересованных сторон распространяются различные нормативно-правовые базы, все они должны, тем не менее, играть важнейшую роль в обеспечении безопасной и защищенной среды для всех лиц, присутствующих на их объектах, будь то посетители, сотрудники, артисты или иные лица.

Ключевые наборы обязанностей и соответствующие рекомендации для операторов объектов включают следующее:

- проведение оценок угроз и факторов уязвимости применительно к конкретному объекту:
  - нужно изучить уязвимость объекта к определенным видам угроз в силу специфических особенностей объекта, его местоположения, размера и т. д., а также изучить уникальные особенности объекта, делающие его уязвимым;
  - следует обратиться к компетентным местным правоохранительным органам за консультацией для понимания текущих угроз и оказать помощь в разработке соответствующих и соразмерных планов обеспечения безопасности;
  - необходимо иметь в виду, что определенные меры эффективно уменьшать одни риски в плане безопасности и быть бесполезными или даже контрпродуктивными в отношении других рисков. Сложной задачей для операторов объектов является обеспечение надлежащего уровня безопасности в условиях многочисленных угроз<sup>39</sup>;
  - необходимо, как подчеркивается в Анталийском меморандуме ГКФ, «проверять предположительные расчеты и внедрить программу анализа извлеченных уроков, в том числе уроков предыдущих нападений»<sup>40</sup>. (ГКФ, 2017 год, пример передовой практики № 11) В то же время анализ, основанный только на прошлых событиях, может быть контрпродуктивным. Вероятно, «мы ожидаем, что группы будут действовать так же, как они действовали в прошлом, и соответствующим образом усиливаем безопасность объектов и осуществляем проверку людей. К сожалению, мы

39 Например, устройство зеленых насаждений в пешеходных зонах может ограничить скорость движения автотранспортных средств, когда они используются для совершения нападений, но может и ограничить способность систем видеонаблюдения фиксировать мелкие преступления.

40 Анталийский меморандум, Пример передовой практики № 11: «...Необходимо применить полученный опыт на местах, а затем продолжать регулярно определять передовые методы и обмениваться опытом в рамках общих усилий. Проведение проверок на уязвимость силами специалистов, которые мыслят как террористы и разрабатывают операции и тактику для выявления слабых сторон противника, может помочь сотрудникам служб безопасности в изучении факторов уязвимости или совершенствовании мероприятий по смягчению последствий и реагированию. В порядке контроля такие специалисты могли бы также тестировать принимаемые службами безопасности меры реагирования».

тратим огромное количество ресурсов на то, чтобы не допустить повторения истории, в то время как группы и отдельные лица, придерживающие-

ся идеологии насилия, изыскивают способы нанести удар по Соединенным Штатам с неожиданной стороны или асимметричным образом<sup>42</sup>»;



Вставка 5.

### **Поощрение разработки планов обеспечения безопасности уязвимых целей с учетом гендерного фактора**

Разработка стратегий уменьшения рисков на институциональном уровне должна включать гендерный анализ и обеспечивать, в частности, условия для того, чтобы при планировании мер по смягчению рисков операторы объектов могли более полно учитывать особые проблемы женщин в плане безопасности и опасения женщин. Обеспечение систематического гендерного анализа может в значительной мере способствовать выявлению факторов, позволяющих смягчить риск, повышению эффективности разработанных стратегий и деятельности по их применению, а также свести к минимуму непропорциональное гендерное воздействие мер по смягчению риска.

- принятие соответствующих мер по смягчению риска:
  - необходимо руководствоваться принципом обеспечения «многоуровневой безопасности» защищаемого объекта. Хотя итоговые меры по смягчению риска могут отличаться по количеству, размаху и степени сложности, принцип обеспечения «многоуровневой безопасности» должен применяться независимо от размеров и сложности соответствующего объекта<sup>42</sup>;
  - нужно рассмотреть весь спектр доступных мер безопасности и определить их наиболее подходящее сочетание на основе результатов оценки безопасности, обязательных/рекомендованных стандартов и наличия бюджетных средств. Кроме того, меры безопасности должны быть соизмеримы с реальной угрозой, а за их применение должны отвечать хорошо обученные и преданные своему делу сотрудники. К числу таких мер относятся следующие:
    - > «физические меры безопасности» (например, наличие охранного персонала, ограждений, камер видеонаблюдения);
    - > «проектные меры безопасности» (т.е. обеспечение безопасности на ранних этапах проектирования объекта);
    - > меры по устранению потенциальной угрозы со стороны лиц, которые пытаются поступить на работу (в качестве сотрудников, добровольцев, временных работников и т.д.) или иным образом получить доступ к объекту (например, в качестве внешних подрядчиков), чтобы получить сведения и/или информацию о внутренней динамике и процессах, которые можно было бы использовать в целях совершения террористического нападения «внутренняя угроза»);
    - > кибербезопасность: растущая зависимость систем от интернета (например, считыватели пропусков, камеры) означает, что террористы могут попытаться «взломать» эти системы, чтобы незаметно получить доступ к объекту;

<sup>42</sup> Многоуровневая безопасность, также именуемая «эшелонированной защитой», подразумевает принятие многоуровневых мер обеспечения безопасности, чтобы в случае несрабатывания одной меры нападение можно было предотвратить или смягчить благодаря эффективности других уровней.

- > средства коммуникации, призванные удержать потенциальных террористов от нападения на объект, в том числе применение средств обмана (например, размещения муляжей камер наблюдения у входа на объект, использования на веб-сайте таких формулировок, которые создадут впечатление, что объект надежно защищен);
- подготовка к чрезвычайным ситуациям:
  - необходимо принять и проверить на практике планы действий в чрезвычайных ситуациях (например, при эвакуации);
  - нужно принять меры для ознакомления компетентных сотрудников правоохранительных органов, служб безопасности и экстренного реагирования с особенностями объекта;
  - необходимо заранее организовать учения, тренировки, инструктажи и т. д. по процедурам действий в чрезвычайных ситуациях (например, в случае эвакуации) для лиц, находящихся на объекте (персонал, посетители и т. д.), при поддержке сотрудников правоохранительных органов и служб экстренного реагирования.



#### Вставка 6.

#### **Безопасность уязвимых объектов: взгляд оператора**

- Меры безопасности должны способствовать ведению коммерческой деятельности, а не препятствовать ей без необходимости. Меры безопасности, основанные на оценке рисков, должны быть соразмерными. Они должны учитывать также, как средства охраны могут влиять на посетителей и как посетители могут на них отреагировать.
- Необходимо разработать соответствующую процедуру проверки, снижающую вероятность проноса запрещенных предметов на объекты и/или в рабочие зоны при сохранении высокого уровня обслуживания посетителей.
- Следует, насколько это возможно, привлекать различных сотрудников к обеспечению безопасности — от специалистов по обслуживанию посетителей до контролеров-распорядителей и сотрудников службы безопасности. Допускается также использование служебных собак.
- Если существует такая возможность, то нужно установить комплексную систему видеонаблюдения, а также систему управления движением транспорта для обеспечения свободного передвижения уполномоченных лиц по территории объекта с учетом их задач и потребностей.
- Необходимо сотрудничать с правоохранительными органами, службами безопасности, органами власти и отраслевыми специалистами, постоянно оценивая и совершенствуя систему действий по обеспечению безопасности.
- Персонал объекта должен быть в достаточной мере подготовлен к реагированию на серьезные происшествия, обладать знаниями и навыками, которые могут потребоваться им самим и для оказания помощи другим лицам в случае серьезного происшествия. Нужно просвещать сотрудников об угрозе терроризма, о том, как они могут помочь предотвратить или отразить нападение, сообщая о подозрительных случаях и соблюдая протоколы безопасности.

*Источник: Counter Terror Business, 2020; Williams, 2021.*



Программный документ 10.

### **Избранные ресурсы для операторов объектов, представляющих собой уязвимые цели, – Министерство внутренней безопасности Соединенных Штатов**

- *Инструментарий и ресурсы в помощь коммерческим структурам для планирования, подготовки и защиты на случай нападения*, в которых предлагаются советы экспертов и рекомендации для частного сектора и партнеров из числа представителей местного населения относительно мер, которые можно предпринять для защиты объектов и мест проведения мероприятий. Коммерческим структурам рекомендуется налаживать взаимосвязь, заниматься разработкой планов и обучением сотрудников и сообщать о возможных инцидентах или готовящихся нападениях, чтобы лучше подготовиться самим и подготовить сотрудников к тому, чтобы они могли заранее продумать, какую роли они играют в обеспечении безопасности и охраны своих структур и сообществ. <https://www.cisa.gov/publication/connect-plan-train-report>
- *Пакет планов повышения устойчивости функционирования*, призванный помочь компаниям в разработке, совершенствовании или обновлении таких планов в целях уменьшения потенциального воздействия помех. Этот пакет планов предусматривает подготовку персонала для составления планов повышения устойчивости функционирования, назначение сотрудников, ответственных за подготовку планов обеспечения бесперебойного функционирования и послеаварийного восстановления, и проведение проверки планов повышения устойчивости функционирования. <https://www.ready.gov/business-continuity-planning-suite>
- *Видео «Check It!» («Проверьте!»)*, содержащее инструкции в отношении правильного досмотра сумок с целью защиты заведений и посетителей. <https://www.cisa.gov/video/check-it-bag-check-video>
- *Руководство по передовой практике досмотра посетителей*, в котором коммерческим структурам предлагаются варианты разработки и внедрения процедур досмотра зрителей на крупных спортивных мероприятиях, концертах, скачках, церемониях награждения и аналогичных массовых мероприятиях. <https://www.cisa.gov/publication/patron-screening-guide>
- *Руководство по планированию действий в чрезвычайных ситуациях, связанных с угрозой нападения с применением огнестрельного оружия*, в котором содержится описание основополагающих концепций разработки планов действий в чрезвычайных ситуациях для сценариев, предполагающих угрозу нападения с применением огнестрельного оружия, включая такие важные аспекты разработки этих планов, как:
  - о демонстрация видео с рекомендациями о важных аспектах разработки планов действий в чрезвычайных ситуациях непосредственно от людей, переживших угрозу нападения с применением огнестрельного оружия, от сотрудников служб экстренного реагирования и других специалистов в этой области, которые рассказывают о своем уникальном опыте; <https://www.cisa.gov/active-shooter-emergency-action-plan-video>
  - о представление информации, необходимой для разработки плана действий в чрезвычайных ситуациях;
  - о представление шаблона в качестве основы для разработки собственного плана действий в чрезвычайных ситуациях для коммерческих структур. <https://www.cisa.gov/publication/active-shooter-emergency-action-plan-guide>

#### Программный документ 10. (продолжение)

- *Руководство по восстановлению после угрозы нападения с применением огнестрельного оружия*, которое призвано способствовать упреждительному внедрению стратегий и процедур, позволяющих организациям эффективно восстанавливаться после инцидента угрозой с применением огнестрельного оружия, предусматривая при этом наиболее оптимальные варианты поддержки сотрудников, подрядчиков, посетителей, клиентов, членов семей и населения в целом. <https://www.cisa.gov/publication/active-shooter-recovery-guide>
- *Практическое руководство для проведения массовых мероприятий: требования к обеспечению безопасности слабозащищенных целей и мест скопления людей*, в котором излагаются некоторые базовые ориентировочные способы, позволяющие коммерческим структурами подготовиться к возможным нападениям и смягчить их последствия, включая охранные меры. <https://www.cisa.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Security%20Awareness%20for%20ST-CP.PDF>
- *Веб-сайт «What to Do – Bomb Threat» («Что делать – угроза взрыва»)*, на котором опубликованы рекомендации и ресурсы, включая подробные процедуры реагирования на угрозы взрыва или порядок действий в случае обнаружения подозрительных предметов или поведения людей, а также информация, помогающая принятию надлежащих подготовительных мер или мер реагирования в таких ситуациях. <https://www.cisa.gov/what-to-do-bomb-threat>
- *Подборка примеров передовой практики Межведомственного комитета безопасности по применению процедур проверки и обработки почтовых отправок*, которая предоставляет управляющим почтовых центров, их руководителям и сотрудникам служб безопасности учреждений рамочные основы для понимания и смягчения рисков для организации, связанных с ежедневными входящими и исходящими почтовыми отправлениями и посылками. <https://www.cisa.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf>
- *Видео «Insider Threat» («Внутренняя угроза»)*, в котором демонстрируются проведенные с участием экспертов по безопасности и поведению обсуждения вопроса о том, как внутренние угрозы проявляются в различных формах, включая терроризм, насилие на рабочем месте и нарушения кибербезопасности. (<https://www.cisa.gov/insider-threat-trailer-and-video>)

#### 4.2.2 Организации гражданского общества

В рамках своих различных сфер деятельности (исследования, политика, взаимодействие с местным населением), основных направлений работы/опыта и деятельности на различных уровнях (местном, национальном, международном) организации гражданского общества (ОГО) могут высказать самые разнообразные ценные замечания по вопросу о защите уязвимых объектов и внести широкий вклад в общие усилия по обеспечению их защиты. Наиболее заметную пользу они могут принести в одной или нескольких следующих областях:

- низовые организации, действующие вблизи от уязвимых целей или осуществляющие проекты в интересах конкретных местных сообществ или районов, могут дать критически важное представление о характере местных угроз. Кроме того, ОГО могут внести свой вклад в разработку планов обеспечения безопасности операторами объектов или государственными органами, как на местном, так и на национальном уровне;
- с точки зрения заблаговременной профилактики террористических нападений ОГО проводят работу и выступают организаторами проектов по дерадикализации и снижению привлекательности насильственного экстремизма





#### Конкретный пример 5. Глобальный фонд для работы с населением и повышения его жизнестойкости

Созданный в 2014 году, Глобальный фонд для работы с населением и повышения его жизнестойкости представляет собой глобальный механизм финансирования, который пользуется поддержкой правительств 19 стран, международных организаций, фондов, корпораций и частных лиц. Его целью является повышение жизнестойкости населения путем предоставления субсидий и поддержки местных инициатив, направленных на устранение факторов, порождающих насильственный экстремизм. Субсидии выделяются юридическим лицам, зарегистрированным на местном уровне, или первичным получателям, которые координируют объединение общинных организаций или суб-получателей, занимающихся проведением мероприятий, направленных на предотвращение насильственного экстремизма. Ускоренное выделение дополнительных средств позволяет оказывать срочную поддержку в порядке реагирования на складывающиеся ситуации.

Выделение средств осуществляется на основании ряда руководящих принципов, включая следующие:

- национальная ответственность: деятельность осуществляется под руководством местных сообществ и направлена на поддержку стратегических целей правительств стран;
- учет существующих условий: решения о выделении средств принимаются на основе тщательной оценки местных факторов, порождающих насильственный экстремизм;
- подотчетность и обучение: методологии и инструментарий постоянно пересматриваются в целях повышения эффективности работы.

Источник: <https://www.gcerf.org/>



Конкретный пример 6.

### **Ликвидация травматических последствий терроризма: миссия Израильского центра травматологии и восстановительного лечения**

Израильский центр травматологии и восстановительного лечения (НАТАЛ) был основан в 1998 году и является неполитической организацией, которая оказывает услуги лицам, получившим непосредственные и косвенные травмы, включая жертв террористических актов. Он обслуживает граждан независимо от их религиозных убеждений, этнического происхождения, цвета кожи, возраста, пола или социально-экономического статуса.

Конкретные задачи НАТАЛ включают следующее:

- обеспечивать многопрофильную помощь по линии своего клинического отдела в составе 150 терапевтов, которые базируются на всей территории страны и предоставляют различные виды эмоциональной поддержки и психологической помощи;
- работать с населением в целом, пропагандируя навыками, позволяющие сохранять эмоциональную устойчивость в условиях постоянных угроз, а также способствовать предотвращению общенациональных чрезвычайных ситуаций и восстановлению после таких ситуаций. Программа работы с населением предусматривает использование выездной бригады для оказания помощи на дому лицам и семьям, которые в силу тяжелых симптомов травмы не могут выйти из дома;
- обеспечивать по линии своего Центра сбор свидетельств очевидцев возможность для ветеранов рассказать на камеру о своем травматическом опыте под наблюдением специалиста по психическому здоровью;
- заниматься повышением степени осведомленности о травмах, связанных с терроризмом, и объяснять, что обращение за психологической помощью не является позором. Отдел по распространению информации о травматических проблемах и по связям с общественностью ежегодно проводит многочисленные кампании и мероприятия, ориентированные на тысячи людей всех возрастов.

Источник: NATAL ([www.natal.org.il/en/](http://www.natal.org.il/en/)).

#### **4.2.3 Частный сектор (кроме операторов объектов)**

«Для того чтобы максимально повысить потенциал защиты слабозащищенных целей, необходимо развивать или укреплять государственно-частные партнерства на всех уровнях государственного управления, включая государственный, местный и региональный уровни. Государствам-членам следует поощрять и поддерживать налаживание с компаниями таких партнерских отношений, которые могут способствовать повышению готовности во всех аспектах, а именно обеспечению защиты от террористических нападений, смягчению последствий таких нападений,

реагированию на них и восстановлению после них, а также расследованию соответствующих инцидентов» (S/2018/1177, приложение, п. 53).

Широкий круг организаций частного сектора играет важную роль в смягчении риска нападений на уязвимые цели, действуя по собственной инициативе, в рамках добровольных государственно-частных партнерств или на основе имеющей обязательную силу нормативно-правовой базы. Приведенные ниже примеры не носят исчерпывающего характера, однако они иллюстрируют многообразие коммерческих структур, которые могут потенциально участвовать в обеспечении защиты уязвимых объектов:



- операторы объектов, представляющих собой уязвимые цели, часто обращаются к услугам частных охранных компаний (ЧОК) для выполнения различных функций, во многом связанных с защитой людей и имущества (например, контролирование доступа на объект, выполнение охранных функций, патрулирование, обеспечение информационной безопасности, консультирование по вопросам модернизации охранных систем). ЧОК, независимо от того, оказывают ли они оперативные услуги или консультативные, могут способствовать обеспечению повышенного уровня безопасности на объектах, работая в тандеме/координации с правоохранительными органами, особенно в странах, которые сталкиваются с высокой террористической угрозой и в которых возможности органов государственной безопасности ограничены. Вместе с тем, чтобы ЧОК могли реально поддерживать общие усилия по защите уязвимых целей, их сотрудники должны пройти надлежащую подготовку. Кроме того, их роли и обязанности должны быть четко регламентированы применимой нормативно-правовой базой и дополнительными кодексами поведения (см. вставку 7). Эффективное регулирование деятельности частных охранных компаний гарантирует не только соблюдение основных профессиональных стандартов их сотрудниками, но и позволяет внести ясность в их отношения с полицией, службами экстренного реагирования и другими государственными органами, в обязанности которых входит защита уязвимых объектов;
- коммерческие структуры, расположенные вблизи уязвимых объектов или поставляющие им товары/услуги, могут внести свой вклад в обнаружение подозрительной деятельности и сообщение о ней. Кроме того, они могут внести вклад в усилия по регулированию кризисов, например, предоставляя убежище людям, эвакуируемым под руководством компетентных правоохранительных и спасательных служб;
- водители и другие сотрудники транспортных компаний, если они прошли надлежащую подготовку, которая позволяет им распознавать подозрительную деятельность и сообщать о ней, зачастую способны вносить более значительный вклад в усилия по предотвращению, поскольку они имеют дело с уличной жизнью и пассажирами своих транспортных средств;



## Вставка 7.

### Международный кодекс поведения частных охранных компаний

Некоторые организации разработали рекомендации и предлагают программы сертификации для обеспечения качества и надлежащего профессионального уровня услуг, предоставляемых частными охранными компаниями. Международный кодекс поведения частных охранных компаний, в частности, был принят в 2010 году на основании инициативы многих заинтересованных сторон, выдвинутой правительством Швейцарии. Хотя предусмотренный в Кодексе механизм носит добровольный характер, в связи с чем он не предназначен для того, чтобы подменить внутренний правовой надзор за деятельностью частных охранных компаний, Кодекс поддерживает усилия по обеспечению того, чтобы при выполнении своих обязанностей ЧОК соблюдали права человека. В частности, подписавшие его компании «заявляют, что они обязуются уважать права человека и выполнять гуманитарные обязательства перед теми, кто оказался затронутым их коммерческой деятельностью, включая персонал, клиентов, поставщиков, акционеров и жителей районов, в которых оказывались услуги. Компании, подписавшие Кодекс, также признают важность уважения разных культур в процессе своей работы, а также лиц, с которыми они контактируют в результате такой деятельности» (Пункт 4 преамбулы).

На сегодняшний день Кодекс подписали несколько сотен частных охранных компаний. Кроме того, Организация Объединенных Наций приняла решение о том, что ее учреждения могут нанимать только тех частных охранников, которые работают в ЧОК, подписавших Кодекс.

В 2013 году было достигнуто соглашение по Уставу Надзорного механизма Кодекса. Надзорный механизм призван «обеспечить эффективное внедрение Кодекса посредством сертификации и мониторинга частных поставщиков охранных услуг, а также посредством принятия процесса рассмотрения жалоб третьих сторон<sup>46</sup>».

- в свете недавних нападений на уязвимые объекты, совершенных с применением арендованных автомобилей, агентства по прокату автомобилей могут принимать меры для пресечения подготовки к таким нападениям, проводя общую проверку в отношении своих клиентов<sup>47</sup>. Аналогичные превентивные меры могут принимать и другие коммерческие структуры, имеющие дело с предметами и материалами двойного назначения, а также поставщики и продавцы беспилотных авиационных систем, которые могут попасть в руки враждебно настроенных субъектов;
- в координации с государственными органами технологические компании могут использовать коммуникационные, геолокационные и алгоритмические возможности своих онлайн-платформ для предоставления услуг пострадавшим сообществам во время разворачивающихся кризисов или на этапе восстановления (см. вставку 7);
- службы общественного питания могут принять меры в целях уменьшения риска того, что террористы могут использовать их для заражения пищи, предоставляемой на такие объекты, как школы, религиозные центры, рекреационно-реабилитационные центры и т. д.

46 URL: [www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-47889.html](http://www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-47889.html).

47 В июне 2021 года Совет Европейского союза принял выводы, в которых рекомендовал государствам-членам «изучить и проанализировать рекомендации и средства по обеспечению безопасности для операторов прокатных транспортных средств с целью предотвращения и смягчения риска нападений с применением транспортных средств в общественных местах» (приложение, пункт. 29).



Вставка 8.

### Средства «Facebook» для оказания помощи в реагировании на кризисы

Раздел «Crisis Response» («Реагирование на кризис») представляет собой центр, обеспечивающий единый доступ к следующим инструментам безопасности «Facebook»:

- **«Safety Check» («Проверка безопасности»):** позволяет пользователям в случае инцидента, затрагивающего район, в котором они находятся, сообщить друзьям и родственникам, что они в безопасности. Эта функция может быть активирована автоматически при наплыве сообщений пользователей и получении подтверждения от стороннего новостного или правительственного источника<sup>48</sup>;
- **«Community Help» («Помощь сообщества»):** позволяет пользователям связаться с другими людьми, находящимися поблизости в пострадавшем районе, чтобы оказать или получить помощь в плане доступа к продовольствию, материалам и убежищу;
- **«Raise Money» («Сбор средств»):** предоставляет собой инструмент для оказания финансовой поддержки пострадавшим от кризиса;
- **«Get Information» («Получение информации»):** содержит ссылки на статьи, фотографии и видео, чтобы помочь пользователям узнать больше о происходящем кризисе, а также о том, как следует реагировать на него или как они могут помочь.

Источник: <https://www.facebook.com/crisisresponse/>

#### 4.2.4 Пользователи уязвимых объектов

Туристы, прихожане религиозных учреждений, посетители известных достопримечательностей в городских центрах и т. д. являются не только потенциальными объектами террористических нападений. Они также являются ключевыми участниками общих усилий по обеспечению безопасности посещаемых ими объектов и ограничению воздействия любых кризисов. В частности:

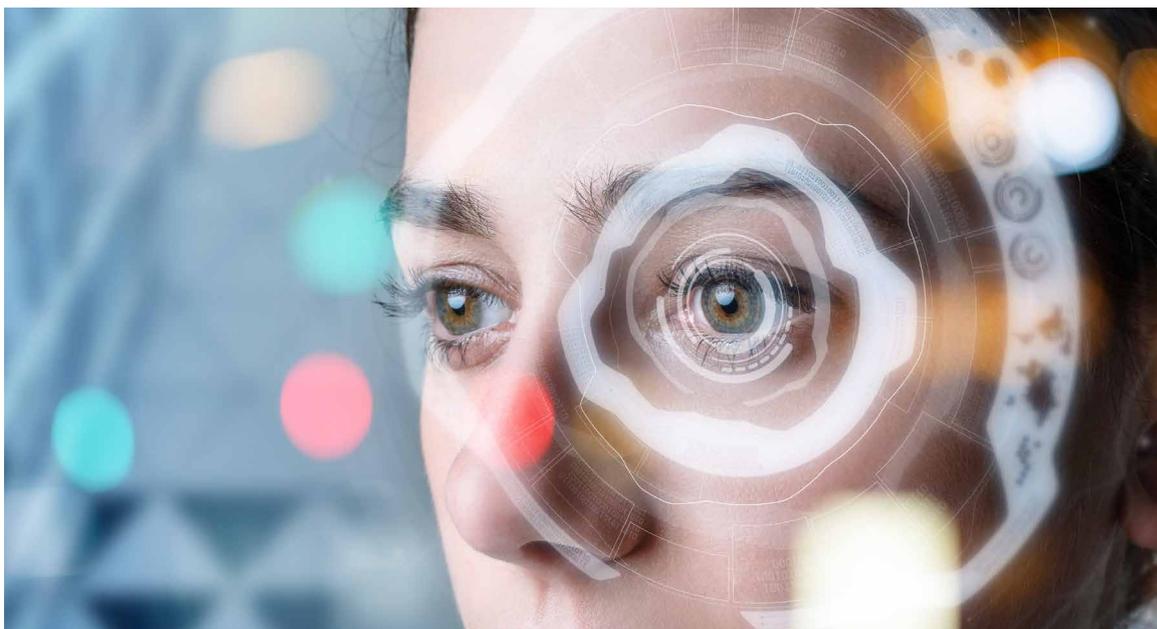
- пользователей уязвимых объектов и население в целом можно научить распознавать необычную активность, включая действия лиц, возможно осуществляющих «предварительное опе-

ративное наблюдение» за объектом, потенциально принимать соответствующие меры и сообщать властям о такой активности. Важность такой подготовки, призванной выявлять подозрительную активность, трудно переоценить, особенно в то время, когда технический прогресс предоставляет потенциальным террористам все более широкие возможности оставаться незамеченными во время наблюдения за целью перед совершением нападения<sup>49</sup>;

- во время кризиса люди, оказавшиеся на затронутом объекте, могут быть в состоянии оказать первую помощь до прибытия сотрудников правоохранительных органов и медицинского персонала. Таким образом, ознакомление

48 Функция проверки безопасности «Facebook» была активирована в связи с нападением, совершенным террористом-смертником в международном аэропорту Кабула 26 августа 2021 года. <https://www.cnet.com/news/facebook-safety-check-activated-after-deadly-attack-outside-kabul-airport/>

49 Например, беспилотные авиационные системы все чаще оснащаются бесшумными двигателями и способны делать детальные снимки с больших расстояний. Кроме того, обычные потребители уже могут приобрести камеры, которые незаметно встраиваются в очки.



тех, кто регулярно посещает определенные уязвимые объекты, с общими навыками оказания первой и неотложной

помощи при травмах может иметь решающее значение для целей смягчения последствий.



Вставка 9.

#### **Последствия для прав человека, порождаемые политикой и практикой, нацеленными на выявление признаков радикализации**

Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом выразил серьезную обеспокоенность по поводу подходов, в соответствии с которыми «обязанности по выявлению «признаков радикализации» возлагаются на различных субъектов общества, включая учителей, социальных работников, медицинский персонал и других работников здравоохранения, сотрудников тюрем, соседей и членов семей, лидеров общин и членов религиозных групп (...) Эти меры не только разрушают хрупкое доверие, которое люди и общины оказывают этим специалистам, чья главная обязанность заключается в том, чтобы обеспечивать защиту и расширять права и возможности, но и, в отсутствие заслуживающего доверия научного понимания процесса, который заставляет людей обращаться к насильственному экстремизму, в значительной мере препятствуют точной идентификации. Такая политика приводит к тому, что под подозрение и в сообщения попадает слишком большое количество людей, в основном на базе запрещенных дискриминационных оснований, что затрагивает права на свободу религии и выражения мнений и неприкосновенность частной жизни».

*Источник: A/HRC/43/46, para. 32.*



Программный документ 11.

**Избранные ресурсы для пользователей объектов, представляющих собой уязвимые цели, – Министерство внутренней безопасности Соединенных Штатов**

- **“If You See Something, Say Something” («Заметил – сообщи»)** – это лозунг национальной кампании, призванной повысить степень осведомленности общественности о признаках терроризма и связанных с ним преступлений, а также о важности сообщения о подозрительной деятельности в правоохранительные органы штата и местные правоохранительные органы; <https://www.dhs.gov/see-something-say-something/about-campaign>
- **в практическом руководстве “Active Shooter Attacks: Security Awareness for Soft Targets and Crowded Places” («Угроза нападения с применением огнестрельного оружия: вопросы безопасности слабозащищенных целей и мест скопления людей»)** перечислены потенциальные угрозы такого нападения, а также шаги, которые необходимо предпринять в случае такого нападения. В нем приводятся полезные советы, которые помогут разработать защитные меры для смягчения последствий будущих нападений; [https://www.fema.gov/sites/default/files/2020-03/fema\\_faith-communities\\_active-shooter.pdf](https://www.fema.gov/sites/default/files/2020-03/fema_faith-communities_active-shooter.pdf)
- **веб-сайт по вопросам обеспечения готовности к нападениям с применением огнестрельного оружия** обеспечивает доступ к ряду продуктов, инструментов и ресурсов Министерства внутренней безопасности, чтобы помочь населению подготовиться к таким инцидентам и принять меры реагирования на них; <https://www.cisa.gov/active-shooter-preparedness>
- **в практическом руководстве “Chemical Attacks: Security Awareness for Soft Targets and Crowded Places” («Химические нападения: вопросы безопасности слабозащищенных целей и мест скопления людей»)** определяются потенциальные сценарии и симптомы возможного воздействия химикатов. Кроме того, в нем разъясняется, как население может реагировать на будущие нападения и смягчать их последствия; ([www.cisa.gov/sites/default/files/publications/Chemical Attacks - Security Awareness for ST-CP.PDF](http://www.cisa.gov/sites/default/files/publications/Chemical%20Attacks%20-%20Security%20Awareness%20for%20ST-CP.PDF));
- **в практическом руководстве “Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places” («Использование автотранспортных средств в качестве тарана: вопросы безопасности слабозащищенных целей и мест скопления людей»)** определяются признаки, по которым можно определить, что те или иные лица планируют совершить нападение с использованием автотранспортного средства в качестве тарана. Кроме того, в нем излагаются предлагаемые стратегии смягчения последствий и возможные защитные меры; ([www.cisa.gov/sites/default/files/publications/Vehicle Ramming - Security Awareness for ST-CP.PDF](http://www.cisa.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF));
- **в практическом руководстве “Mass Gatherings: Take Charge of Your Personal Safety” («Массовые мероприятия: обеспечение личной безопасности»)** излагаются потенциальные признаки готовящегося нападения на место проведения массового мероприятия и определяются возможные меры реагирования со стороны населения. ([www.cisa.gov/sites/default/files/publications/Mass Gatherings - Take Charge of Your Personal Safety.pdf](http://www.cisa.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Take%20Charge%20of%20Your%20Personal%20Safety.pdf)).



## Справочные материалы

Australia-New Zealand Counter-Terrorism Committee (ANZCTC), 2017. Australia's Strategy for Protecting Crowded Places from Terrorism ([www.nationalsecurity.gov.au/crowded-places-subsite/Files/australias-strategy-protecting-crowded-places-terrorism.pdf](http://www.nationalsecurity.gov.au/crowded-places-subsite/Files/australias-strategy-protecting-crowded-places-terrorism.pdf)).

Counter Terror Business (CTB), 2020. The O2 and event security, interview (February) (<https://counterterrorbusiness.com/features/ctb-interview-o2-and-event-security>).

Geneva Centre for Security Sector Governance (DCAF), OSCE Office for Democratic Institutions and Human Rights (ODIHR) and UN Women, 2019. *Policing and Gender, Tool 2, Gender and Security Toolkit*.

\_\_\_\_\_, 2019. *Intelligence and Gender, Tool 14, Gender and Security Toolkit*.

Global Counterterrorism Forum, 2017. Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context ([www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth GCTF Coordinating Committee Meeting/GCTF - Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context.pdf?ver=2017-09-17-010844-720](http://www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/TwelfthGCTF%20Coordinating%20Committee%20Meeting/GCTF%20-%20Antalya%20Memorandum%20on%20the%20Protection%20of%20Soft%20Targets%20in%20a%20Counterterrorism%20Context.pdf?ver=2017-09-17-010844-720)).

Hesterman, Jennifer, 2019. *Soft Target Hardening: Protecting People from Attack*. Routledge.

Organization for Security and Cooperation in Europe (OSCE), 2014. Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach.

Swedish Civil Contingency Agency (MSB), 2011. A first step towards a national risk assessment: National risk identification ([www.msb.se/siteassets/dokument/publikationer/english-publications/a-first-step-towards-a-national-risk-assessment--final.pdf](http://www.msb.se/siteassets/dokument/publikationer/english-publications/a-first-step-towards-a-national-risk-assessment--final.pdf)).

United States of America, Department of Homeland Security (DHS), 2018. *Soft Targets and Crowded Places Security Plan Overview* ([www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508\\_0.pdf](http://www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf)).

United States of America, Government Accountability Office (GAO), 2012. Nuclear Nonproliferation: Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities ([www.gao.gov/assets/gao-12-925.pdf](http://www.gao.gov/assets/gao-12-925.pdf)).

Williams, Paul, 2021. Intervention by Head of Security at AEG Europe, at the UNOCT-organized Nations Expert Group Meeting (EGM) on the Protection of Urban Centers and Tourist Venues (15 and 16 June) (see [www.un.org/counterterrorism/events/international-expert-group-on-protection-urban-centres-touristic-venues](http://www.un.org/counterterrorism/events/international-expert-group-on-protection-urban-centres-touristic-venues)).



Дополнительная информация представлена на веб-сайте:  
[www.un.org/counterterrorism/vulnerable-targets](http://www.un.org/counterterrorism/vulnerable-targets)



КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ  
ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ