Обеспечение безопасности критических инфраструктур в США (аналитический обзор)

В. Н. Цыгичко, Г. Л. Смолян, Д. С. Черешкин

Настоящий обзор составлен на основании директивных документов, регламентирующих деятельность органов государственного управления США различных уровней по обеспечению безопасности критически важных объектов инфраструктур, опубликованных в открытой печати. Список использованных источников приводится в конце обзора.

Введение

В последние годы западные специалисты, признавая возможность прямой угрозы нанесения ядерных ударов по территории США, Западной Европы и Японии, уделяют особое внимание оценке воздействия по жизненно важным объектам своих стран неядерными средствами и возможных последствий этих воздействий для политической, экономической, экологической и других сфер деятельности государства. Очевидно, что в условиях современного чрезвычайно интенсивного развития инфраструктуры ведущих зарубежных стран существует множество так называемых критически важных объектов (КВО), таких, например, как крупные гидротехнические сооружения, нефте-, газо-, продуктопроводы, сети АЭС, пункты хранения стратегических запасов нефти и газа, вредные химические производства, транспортные узлы, аэродромы и т. п., выведение из строя которых может привести к непредсказуемым тяжелым и даже катастрофическим последствиям.

В связи с этим в Соединенных Штатах, Франции, Германии, Японии и других странах были проведены обширные исследования по выявлению таких объектов как на территории США и Канады, так и в Европе, включая Россию, представляющих угрозу для нормальной жизнедеятельности рассматриваемых стран в случае воздействия по ним безъядерного высокоточного оружия или в результате террористических (диверсионных) актов. Также прорабатывались варианты техногенных катастроф или разрушительных стихийных бедствий.

1. Критически важные объекты и обеспечение национальной безопасности

В предлагаемом обзоре в перечень выявленных критически важных объектов (КВО) не включены традиционные типы военных объектов — ракетные базы и полигоны, авиационные базы, органы высшего государственного и военного управления, так как по оценкам исследователей эти объекты имеют достаточно высокую степень защищенности и практически являются мало уязвимыми от воздействия обычных средств поражения. Кроме того, даже вывод из строя подобных объектов не нарушит существенно системы жизнеобеспечения государства и его управляемость.

Главную угрозу для жизнедеятельности страны представляет выведение из строя объектов, приводящее к нарушению транспортных и энергетических систем, водоснабжения и др. в масштабах страны или отдельных районов. По результатам исследования на территории США и Канады выделено около 2 300 подобных объектов, в Германии — более 650, Франции — около 500, в Японии — до 700. При этом отмечается, что они обладают относительно низкой защищенностью и имеют большое количество уязвимых точек «несанкционированного доступа», воздействие на которые может привести фактически к полному параличу систем жизнедеятельности государства. В первую очередь к таким объектам относятся крупные гидротехнические сооружения (оценочно их насчитывают более 60), разрушение которых может привести к затоплению больших территорий и даже отдельных государств.

На территориях США и Канады выделены: 16 водохранилищ и плотин, более 25 атомных электростанций, свыше 70 хранилищ стратегического нефтяного резерва, около 120 крупнейших автоматических коммутационных центров сетей связи и значительное количество других подобных объектов.

Были сделаны следующие выводы:

- в условиях современного интенсивного развития инфраструктуры и полной зависимости населения от систем жизнеобеспечения проведение крупномасштабных вооруженных конфликтов с применением как обычных средств поражения, так и массированного использования ядерного оружия, становится бессмысленным из-за угрозы полного самоуничтожения противоборствующих сторон, так как последствия разрушений «узловых» элементов инфраструктуры (даже одиночных) приводят к непредсказуемым последствиям;
- для прекращения нормального функционирования одного или нескольких государств в Центральной Европе достаточно осуществить подрыв (военным или диверсионным способом) нескольких десятков КВО, причем выведение из строя АЭС и гидросооружений будет иметь наиболее долговременные последствия;

- существующие методики оценки поражающих факторов ядерного взрыва (за исключением избыточного давления во фронте ударной волны) оказались практически несостоятельными и требуется разработка новых подходов к оценке последствий других факторов, особенно радиоактивного заражения местности (на опыте реактора Чернобыльской АЭС);
- необходимо в кратчайшие сроки разработать методы оценки «… последствий непредсказуемого поведения АЭС в случае их затопления водными массами» и комплекс мер по их ликвидации;
- рост боевых возможностей неядерного высокоточного оружия позволяет использовать его для уничтожения ядерного потенциала государств в условиях безъядерного конфликта и это существенно повышает риск ответного применения ядерного оружия, когда возникает угроза уничтожения этого потенциала.

2. Критерии выделения КВО

К критически важным объектам (КВО), которые составляют критически важную инфраструктуру, относятся:

- системы сельскохозяйственного и продовольственного обеспечения;
- финансово-банковская система (потери в сфере финансово-банковской системы из-за компьютерных атак ежегодно составляют более 10 млрд долл.);
- транспортная система;
- система водоснабжения (ежегодно для обеспечения безопасности на таких объектах выделяется более 90 млн долл.);
- службы спасения и оказания скорой помощи;
- система энергоснабжения;
- система государственного управления.

В США принято подразделять КВО на объекты инфраструктуры, связанные с международными организациями (объекты энергетики, транспорт, банковско-финансовая система, телекоммуникации) и несвязанные (водоснабжение, службы спасения, государственное управление).

Исходя из анализа взглядов руководства США, определены три категории КВО:

Жизненно важные:

- АЭС;
- ГЭС (более 2 Гватт);

- гидротехнические сооружения;
- объекты хранения стратегических запасов нефти и газа;
- вредные химические и нефтехимические производства (помимо террористических атак подвержены техногенным катастрофам). Только в США в 90-е гг. прошлого столетия из-за катастроф погибло 182 человека и ранено более 2 000 человек, в сравнении с тем, что от террористических проявлений соответственно 23 и 105 человек. Около 41 млн американцев живет в непосредственной близости от нефтехимических и других вредных производств — «зоне уязвимости», при этом зона опасности для токсических производств составляет около 3 км, а для производств легковоспламеняющихся средств — примерно 800 м. Однако для некоторых производств эта зона составляет до 20 км, для безводного аммиака, фтористоводородных продуктов, сернистого ангидрида и ряда других — 20–40 км. В соответствии с проведенными оценками в среднем для токсичных производств авария уносит жизнь 15 человек, а для производств легковоспламеняющихся средств — более 1 500. В США около 15 тыс. опасных объектов, из них 123 завода, которые в случае аварии представляют угрозу более 1 млн человек., более 700 — для городов с населением более 100 тыс. человек, более 1 700 — для населения более 1 000 человек. При изучении обстановки на 14 500 объектах было отмечено 1 913 аварийных ситуаций на 1 145 объектах, в половине случаев пострадали люди, для устранения последствий были привлечены более 200 тыс. человек. Проведенные расчеты показали, что при нападении на крупнейшее американское производство могут пострадать до 2,5 млн чел. Для обеспечения безопасности химических производств в 2003 г. было выделено 10 млрд долл., для проведения оценки уязвимости выделяется более 80 млн дол в период 2005–2009 гг.;
- склады хранения ядерных материалов и боеприпасов.

Крайне важные:

- системы энергообеспечения (более 2 Гватт);
- метрополитен;
- линии водоснабжения;
- подземные канализационные системы (в 2004 г. для обеспечения безопасности таких систем выделено 180 млн долл., для проведения исследований в области оценки их уязвимости выделено 22 млн дол, полномасштабное планирование мероприятий по обеспечению безопасности предполагается для всех установок, рассчитанных на обслуживание более 25 тыс. человек);
- магистральные трубопроводы (более 100 млрд кубических метров).

Важные:

- морские порты (в США более 300 крупных морских и речных портов с более чем 3 700 грузовыми и пассажирскими терминалами, более 1 000 других портовых сооружений, при этом 50 крупнейших портов обеспечивают транспортировку до 90 % всех грузов, а 25 портов — 98 % всех контейнерных перевозок. В США ежегодно заходит более 5,5 тыс. судов, которые в течение года производят более 60 тыс. заходов в порты. Судами обеспечивается перевозка до 80 % всего объема торговли, которая дает США до 25 % всего валового внутреннего продукта, нарушение перевозок может привести к значительному экономическому кризису, закрытие порта на одни сутки приводит к потерям до 1 млрд долл. 17 портов имеют стратегическое значение и используются совместно министерством транспорта и министерством обороны. Во время войны в Ираке 90 % всех грузовых переброс проведены морским путем из 18 портов. Помимо террористов, угрозу представляет криминал, ежегодно в США в портах расхищается продукции на 10–15 млрд долл.);
- очистные сооружения;
- магистральные сооружения (в США около 7 млн км дорог, из них более 80 тыс. магистральных, более 600 тыс. мостов. Протяженность железных дорог составляет около 550 тыс. км;
- крупные аэропорты (более 500 крупных аэропортов и более 14 тыс. малых аэропортов и площадок;
- крупные центры связи;
- магистральные трубопроводы.

Департамент информационного анализа и защиты инфраструктуры Министерство внутренней безопасности (МВБ) США выделил и включил в создаваемую общенациональную базу данных около 33 тыс. КВО. В соответствии с имеющимися планами вокруг каждого объекта должна быть создана буферная зона безопасности.

3. Система обеспечения безопасности КВО США

Защита критически важных объектов (КВО) и их совокупности, которую принято называть критически важной инфраструктурой, или, короче, критической инфраструктурой, представляет собой одну из наиболее важных задач обеспечения национальной безопасности любой страны. Защита КВО включает проведение мероприятий, которые должны обеспечить их сохранение в случае различных воздействий природного или техногенного характера. Наибольшую опасность по мнению руководства ведущих зарубежных государств в настоящее время представляет терроризм. Опыт

последних событий в мире показывает, что опасность терроризма постоянно возрастает.

Трудности борьбы с терроризмом определяются следующими факторами:

- обычные боевые действия являются полной противоположностью асимметричных действий террористов;
- как правило, организационная структура террористических организаций не позволяет ее быстро обнаружить и оперативно ликвидировать;
- идентификация правонарушителей часто затруднена;
- доктрина терроризма межнациональна и оппозиционна государственной власти;
- цепочка связей внутри террористических организаций запутана и аморфна;
- масштабы материально-технического снабжения террористов относительно невелики, что затрудняет их отслеживание;
- требования по обнаружению отдельных бойцов и разведке баз террористов в различных условиях могут значительно отличаться.

Наиболее развитая система борьбы с терроризмом и защиты КВО создана в США. Она включает разработку необходимой законодательной и юридической основы, весьма значительный объем финансирования, образование необходимых органов управления и подчинение им чрезвычайных служб, оснащение необходимыми техническими и программными средствами. Во многом система обеспечения безопасности КВО становится объектом изучения и примера для других государств, создающих аналогичные системы с учетом национальных особенностей, традиций и особенностей государственного устройства.

Для решения задач управления кризисами в США создана система стратегического руководства, которая в структурном плане представляет собой организационно-техническое единство высших государственных и других органов, технических систем и средств управления и связи, обеспечивающих деятельность политического руководства по управлению страной.

Оперативное управление страной осуществляется посредством ***общей системы управления***.

В состав системы входят:

- национальная система оперативного управления;
- системы управления и связи территориальных органов;
- информационно-вычислительные системы негосударственных объединений;
- системы управления и связи агентств и ведомств США.

Система управления безопасностью США строится как открытая, иерархическая, многоуровневая сложная система, имеющая единый управ-

ляющий орган (Белый дом) и управляемые объекты вплоть до органов местного управления. Она обеспечивает:

- получение вышестоящими органами всей необходимой информации от любого подчиненного или взаимодействующего органа (пункта) управления, находящегося в любой точке страны;
- автоматизированную подготовку данных для оперативного планирования и принятия решения на применение имеющихся сил и средств, в том числе в составе сводных групп;
- техническую совместимость систем связи и автоматизированную обработку данных всех ведомств и сбор информации в масштабе времени, близком к реальному;
- автоматизированную обработку и доведения до потребителей всей генерируемой информации (включая разведывательную), необходимой для оперативного планирования и принятия решения;
- сопрягаемость на всех уровнях звеньев управления; закрытие и защиту информации; циркулярное вещание и обработку запросов потребителей на информацию.

Основными элементами системы обеспечения безопасности являются:

1. Управляющие пункты и центры, функционирующие как в дежурном режиме.
2. Системы предупреждения, осуществляющие информирование руководства США и оповещение различных органов об угрозе атак на КВО.
3. Системы связи общего и специального назначения, предназначенные для передачи указов и распоряжений, информации и проведения телеконференций.
4. Вычислительные сети, обеспечивающие информационные потребности абонентов системы для оценки обстановки и принятия решений на различных уровнях.
5. Средства отображения информации для наглядного представления донесений и организации взаимодействия систем, входящих в общую систему, позволяющие осуществлять подключение к нужным системам, ввод и получение данных по запросам и их наглядное отображение.

Каждый из перечисленных элементов действует на различных уровнях государственного управления, а все вместе они образуют информационную систему глобального охвата.

Основными принципами создания системы являются:

- единое представление обстановки во всех звеньях системы управления;
- возможность получения видео, аудио или графической информации с любого терминала системы из глобально распределенных баз данных;

- возможность организации автоматизированной высокоскоростной передачи данных между любыми средствами автоматизации управления, в том числе и входящими в состав информационных систем различных органов в совместной операции;
- непосредственная передача данных о чрезвычайной ситуации в любую точку.

Система оперативного управления безопасностью США формируется на базе технических средств государственной информационной инфраструктуры и прикладного программного обеспечения, необходимого для автоматизации функций по управлению силами и средствами.

По результатам анализа событий 11 сентября 2001 г. в США были сделаны выводы о том, что теракты можно было предотвратить, в случае если бы вся информация была заранее обобщена и проанализирована. Если в 2001 г. ***Федеральному агентству по чрезвычайным ситуациям*** (ФЕМА) на борьбу с терроризмом было выделено около 34 млн долл., при этом 2/3 всех расходов приходились на органы местной власти, то в 2002 г. расходы выросли более чем на порядок и оцениваются не менее, чем в 3,5 млрд долл. Министерству обороны США выделяется до 8 млрд долл. на решение задач внутренней безопасности и организации помощи гражданским органам власти. В январе 2003 г. решением администрации президента США в разведывательном сообществе был создан ***Интеграционный центр террористических угроз***. На защиту КВО в 2001 г. выделялось около 2 млрд долл., после 2001 г. вероятно не менее 25–30 млрд долл.

В октябре 2001 г. после известных событий в Нью-Йорке президент США подписал указ о создании ***Министерства внутренней безопасности*** (МВБ) — общегосударственного органа, который должен обеспечивать координацию всех усилий по защите внутренней территории и защиты КВО. Роль МВБ аналогична роли СНБ в сфере внешней политики и основными функциями являются управляющая и координирующая. В состав министерства вошли более 22 федеральных агентств, ведомств и отдельных структур с общей численностью около 170 тыс. человек. Бюджет нового ведомства составляет около 40 млрд долл. (в 2003 г. — 37,4 млрд долл.).

В своей работе МВБ плотно взаимодействует с другими органами — правоохранительными, разведывательными и ведомственными.

Деятельность МВБ регламентируется Законом о национальной безопасности 2002 г. (107–296), который определяет следующие основные задачи данного органа:

- предотвращение террористических атак на территории США;
- снижение уязвимости США со стороны террористических проявлений;
- минимизация ущерба и потерь и помощь в восстановлении жизнедеятельности и функционирования государства при совершении террористических атак;

- выполнение функций координирующего органа при планировании действий в условиях природных катаклизмов и техногенных катастроф;
- руководство и контроль за деятельностью органов и департаментов внутри ведомств, связанных с обеспечением безопасности, при условии, если их деятельность не оговорена специальными законодательными актами Конгресса;
- обеспечение экономической безопасности государства;
- контроль и нарушение связей между нелегальными организациями, связанными с наркоторговлей и терроризмом;
- обеспечение приграничной безопасности, транспортного сектора, портов, критически важной инфраструктуры и объектов;
- обобщение и анализ информации, поступающей от различных органов и ведомств и связанной с обеспечением внутренней безопасности;
- координация связей между органами государственного и местного управления, частным сектором и гражданами, касающихся возникающих угроз и подготовки к реагированию на них;
- координация усилий правительственных органов по защите граждан от биотерроризма и другого оружия массового поражения;
- помощь в подготовке и обучении служб и персонала, предназначенного для реагирования в чрезвычайных ситуациях, в том числе с применением распределенных по территории США сетей;
- руководство деятельностью государственных спасательных служб.

В МВБ имеется четыре основных департамента:

- приграничной и транспортной безопасности;
- подготовки к чрезвычайным ситуациям и реагирования;
- научно-технологический;
- информационного анализа и защиты инфраструктуры.

Внутренняя безопасность в США включает следующие основные области:

- разведка и оповещение;
- приграничная и транспортная безопасность;
- контртеррористическая борьба внутри страны;
- защита критически важной инфраструктуры и объектов;
- защита от угроз катастроф;
- подготовка к чрезвычайным ситуациям и реагирование.

Особенностью американской системы является высокая степень кооперации и включение органов военного управления для решения поставленных задач. Военные объекты относятся к важным и критически важным

объектам, а силы и средства МО США задействуются как для доведения информации о происшествиях и чрезвычайных ситуациях, так и для устранения угроз и ликвидации последствий происшествий и катастроф, для чего организованы специальные группы взаимодействия с гражданской администрацией на различных уровнях от федерального до местного. Для решения задач внутренней безопасности организуется взаимодействие с министерством обороны, в состав которого с 1 октября 2002 г. было включено новое североамериканское командование, а также утвержден пост помощника министра обороны по внутренней безопасности. Деятельность помощника министра обороны по внутренней безопасности регламентируется ***Законом о национальной обороне*** **(107–314)**, который определяет его обязанности:

- проведение стратегического планирования деятельности МО США по вовлечению в решение задач внутренней безопасности;
- проведение подготовки к обеспечению поддержки гражданских органов различного звена;
- обеспечение взаимодействия и контроль процесса сопряжения систем связи;
- поддержка технологического обеспечения разработок систем и средств.

Североамериканское командование в рамках взаимодействия призвано выявлять, предотвращать и ликвидировать угрозы и агрессивные действия против государства и граждан, при этом зона действия включает, помимо территории США, Канаду и Мексику. Силы данного командования должны обеспечивать поддержку более 79 тыс. муниципальных органов, расположенных по всей территории США, которые могут стать объектами стихийного бедствия или террористической атаки. Наиболее важным элементом является при этом ***Национальная гвардия сухопутных войск США***, которая находится в двойном подчинении — МО США и губернатора штата. Взаимодействие производится через специально организованные в Национальной гвардии группы поддержки гражданских органов.

Решающую роль в функционировании системы обеспечения безопасности играет ***департамент информационного анализа и защиты инфраструктуры МВБ*** США. Основные усилия департамента направлены на:

- определение и оценку угроз (разработка средств и методов моделирования террористических организаций, выявление возможностей террористов, интеграция и корреляция всей информации и последующий анализ);
- определение критически важных объектов и инфраструктуры (выявление КВО, оценка потенциальных рисков проведения успешных атак на них, определение приоритетов при разработке мер защиты);
- оценка уязвимости инфраструктуры (работа специальных экспертных групп, которые командируются для работы на КВО для оценки их уязвимости);

- защита инфраструктуры и КВО (работа выделенных лиц для организации помощи по снижению рисков в государственных и местных органах и частном секторе, включающая обучение, подготовку и планирование мероприятий по защите и реагированию, разработка важнейших программ, технологическая помощь, распространение опыта работы);
- анализ рисков для национальной инфраструктуры (работа по обеспечению объектов национального масштаба, анализ угроз общего характера, при этом целью является обеспечение оперативной, обоснованной информации, понятной для промышленных кругов);
- ведение баз данных по угрозам, уязвимостям и объектам (разработка, организация и поддержка интегрированных баз и серверных устройств, обеспечивающих хранение информации по угрозам, рискам, слабым местам в системах защиты применительно к оборудованию и объектам, включая вероятность атак и связанных с ними ущербов);
- конкурсный анализ и оценки (обеспечение деятельности специальных комиссий и лиц, призванных оценить эффективность продукции и мероприятий по защите объектов, в рамках данной программы предполагается создание «красных команд», которые должны обеспечивать проведение испытаний, учений, игр, альтернативного анализа гипотез и оценку действий).

Ежегодно в США, помимо учений и тренировок на уровне штатов и местных органов управления, проводится 4–5 крупных учений федерального уровня, призванных обеспечить проверку реальности и реализуемости планов развертывания штабов и пунктов управления по действиям в чрезвычайных ситуациях, оценку готовности выделенных сил и технических средств, системы управления и связи, а также степень взаимодействия различных экстренных служб и их способность к выполнению поставленных задач в заданных объемах и в установленные сроки. В ходе таких учений отрабатываются, как правило, действия по какому-либо сценарию, которые требуют совместного участия различных ведомств и органов. Численность ежегодно проводимых учений на том или ином уровне и с использованием различных средств, возросла до более 200 в год, при этом используются как компьютерные игры и штабные тренировки, так и полномасштабные учения с реальным привлечением различных органов, сил и технических средств.

Приоритетами для американской системы обеспечения безопасности КВО являются:

- сохранение жизни и минимизация риска для здоровья граждан;
- предотвращение угроз со стороны террористов;
- обнаружения пребывания, оценка степени готовности к применению, контроль перемещения оружия массового поражения;

- обнаружение, обеззараживание и дезактивация, транспортировка и уничтожение опасных веществ, предотвращение вторичных эффектов таких веществ;
- публичное распространение информации от любых представительных органов и ведомств, отвечающих за реагирование, о возникающих угрозах, о чрезвычайных ситуациях посредством необходимых адекватных и надежных систем и средств связи;
- сохранение и подготовка необходимых средств обеспечения безопасности и восстановления;
- проведение мероприятий по восстановлению объектов.

В соответствии с планом организации взаимодействия чрезвычайных служб установлен перечень уровней опасности, который разработан ФБР и служит для определения характера и масштабов реагирования федеральных служб на появляющиеся происшествия и угрозы их возникновения. Каждый уровень характеризует расширяющийся круг действий, который будет применен в том или ином случае кризисной ситуации. Федеральное правительство при необходимости может при этом доводить информацию о своих действиях и координировать их с правительственными органами штатов и органов местного управления.

В настоящее время в США принята следующая система иерархии уровней угроз:

1. № 4 (*Минимальная угроза*), полученные угрозы не влияют на функционирование органов, объектов и ресурсов (все ведомства действуют в повседневном режиме).
2. № 3 (*Потенциальная угроза*), разведывательные или другие источники показывают, что возникла потенциальная угроза террористического нападения, однако она не рассматривается как неизбежная.
3. № 2 (*Вероятная или правдоподобная угроза*), проведенные оценки угрозы подтверждают возможность наличия у террористов оружия массового поражения и вероятность его применения. На этом уровне угрозы ситуация требует проверки готовности сил и ресурсных средств к реагированию на чрезвычайную ситуацию с целью предотвращения или предупреждения. Федеральные органы сосредотачивают свое внимание на законодательных аспектах действий, которые будут проводить, мероприятий по обеспечению безопасности и процветанию нации. Проводится подготовка и моделирование возможных действий при развитии ситуации по тому или иному сценарию.
4. № 1 (*Чрезвычайная ситуация*), произошел террористический акт или природный катаклизм, который требует немедленного проведения идентификации, оценки и планирования процесса использования федеральных ресурсов и согласованной работы органов различного

уровня, привлечения ресурсов для снижения до минимума последствий происшествия. При этом предполагается наличие жертв в различном масштабе и ставится задача снизить их количество.

Обеспечение надежного и оперативного управления системой безопасности является основной задачей, которая определяется заблаговременно на этапе повседневной деятельности и описывается в предварительных распоряжениях и планах реагирования на чрезвычайные ситуации. Управление осуществляется с учетом особенностей исторически сложившейся управленческой структуры того или иного уровня, ведомства или штата в зависимости от сложности ситуации, имеющихся возможностей и ресурсов. Действия систем управления государственного, уровня штатов и местного обязательно согласуются и учитывают гибкость реагирования на ситуацию для оптимального распределения сил и средств по объектам и времени. Значительное внимание уделяется интеграции систем различного уровня и использованию всех преимуществ, которые дает каждая из них.

Немаловажное значение имеет, по взглядам западных специалистов, организация управления по борьбе с последствиями чрезвычайных происшествий. Системы штатов и местных органов власти обычно включают в свой состав модульные функционально ориентированные группы, которые соответствуют по своим типам, масштабам и потребностям наиболее вероятным инцидентам. Как правило, такие группы многофункциональны и мобильны. Планы органов власти в штатах и на местах обычно определяют перечень действий и процедуры для действий в случае происшествий на тех или иных КВО. Организационная структура штаба руководства строится по иерархичному принципу управления с распределением обязанностей и подчинением всех руководителю по кризису, который определяет, какие ресурсы необходимо задействовать. Группа реагирования в некоторых случаях будет трансформироваться в объединенный штаб, который будет включать различные компоненты (секции, группы) и руководство) и размещаться на ***Специальном пункте управления действиями в чрезвычайной обстановке*** (EOC — Emergency Operations Center), оснащенном различными средствами управления и связи и обеспечивать работу специалистов из различных ведомств разного уровня. Такой пункт управления будет подключаться к информационным сетям и взаимодействовать с вышестоящими органами, обеспечивая информирование по обстановке и проведение запросов.

Общее руководство и ответственность за проводимые мероприятия несет губернатор штата.

ФБР развертывает самостоятельную группу из специально подготовленных агентов в соответствии с масштабами кризисной ситуации, которая координирует свою работу с местными органами (органами штатов) управления и правопорядка.

При совместной работе основное внимание уделяется координации усилий различных органов и ведомств, а также трех уровней государственной власти, так как неизбежно возникают две линии разрешения ситуации, одна из которых проходит по линии государственного управления через прокурора и губернаторов, а вторая по линии чрезвычайных служб, что требует дополнительной координации. На национальном уровне ФБР отслеживает ситуацию и аккумулирует всю информацию в своем штабе и в Центре стратегической информации и операций.

Роль ФБР заключается:

- в оценке точности и достоверности информации;
- инициации процесса оценки угрозы;
- оповещении других ведомств, отвечающих за реагирование;
- оповещении органов власти на всех уровнях в части, их касающейся.

МВБ выполняет:

- предложения ФБР по действиям в складывающейся обстановке;
- проверку получения информации местными органами;
- оповещение других органов.

Вся информация по вопросам национальной безопасности, поступающая в Белый дом, сосредотачивается в центре слежения за обстановкой (ЦСО). ЦСО является основным оперативным органом президента в чрезвычайных условиях и в кризисных ситуациях мирного времени, работой которого руководит помощник президента по национальной безопасности.

В рамках МВБ действует в непрерывном дежурном режиме центр управления, на котором постоянно находится дежурная смена, отвечающая за прием сигналов оповещения об опасности и принятие экстренных мер.

Для эффективного функционирования системы обеспечения безопасности КВО необходим непрерывный и последовательный мониторинг угроз, связанных с возможным проведением терактов, с постоянной и достоверной оценкой возможностей противодействия, нейтрализации и предотвращения этих угроз. В целом мониторинг должен охватывать:

- динамику ситуации, глобальные и локальные противоречия и конфликты;
- научно-технический прогресс в области разработки средств и методов воздействия на физическую и информационную инфраструктуру, а также в области защиты информации;
- состояние внутреннего и международного законодательно-правового обеспечения информационной безопасности;
- состояние и эффективность систем обеспечения как физической, так и информационной безопасности.

Идеальную схему организации мониторинга можно представить в виде иерархической структуры, высшим звеном которой является надведомственный полномочный орган, куда от министерств, ведомств и собственных источников поступает информация о состоянии безопасности объектов и систем. Анализ этой информации позволит оценивать и прогнозировать ситуацию по обеспечению безопасности, осуществить координацию деятельности и сформировать планы развития системы безопасности в целом. Реализация подобной схемы мониторинга в настоящее время затруднена, так как обеспечением безопасности сегодня вынуждены заниматься различные государственные ведомства, прежде всего силовые министерства. Чтобы такого рода «мозаичный» конгломерат отдельных ведомственных подсистем функционировал успешно и эффективно, должны быть согласованы их усилия и скоординирована их деятельность, прежде всего, на нормативно-правовом и методическом уровнях.

Важное место в системе обеспечения защиты КВИ играет министерство здравоохранения, которое отвечает за обеспечение противодействия биотерроризму. Министерство получило на проведение соответствующих работ в области обеспечения внутренней безопасности в 2003 г. 3,1 млрд долл., в том числе на опережающее развитие системы оповещения о биологических угрозах (на оснащение систем безопасности на уровне штатов и местных органов выделяется примерно 2 млрд долл.). После 2001 г. рост финансирования исследовательских лабораторий увеличился почти в 15 раз (с 15 до 120 млн долл.). Сеть специализированных лабораторий охватывает всю территорию США, включая удаленные районы. В первую очередь внимание уделяется техническому оснащению, которое позволяет повысить оперативность выявления чрезвычайной ситуации и провести оповещение.

4. Принципы и порядок функционирования системы обеспечения безопасности КВО

Системы обеспечения безопасности КВО в различных странах функционируют на основании одних и тех же принципов, при этом порядок их функционирования также имеет много общих черт и признаков. Различия определяются выбранными приоритетами и особенностями внутреннего устройства государства, при этом важную роль играет оценка руководством страны перечня угроз и их масштабов. В Европейских странах исторически сложилась более мощная полицейская система на местном уровне, большое внимание уделяется техногенным катастрофам. В Японии существенным признаком является наличие неблагоприятного во многих отношениях климата, постоянных цунами и других стихийных бедствий, наличие атомных электростанций, горный рельеф в сочетании с сейсмической активностью.

Однако даже в этой стране система становится во многом похожа на американскую, что обусловлено, во-первых, участием японской стороны в операции в Ираке и непрерывными угрозами со стороны исламских фундаменталистов в адрес руководства страны и населения, а также появлением и активизацией внутринациональных групп, подобных секте Аум-Синрикё. Таким образом, перечень угроз и вероятность их осуществления во многих странах примерно равны. США, обладая несравнимо более значимыми финансовыми и материальными ресурсами, сумели развернуть и поддерживать в готовом состоянии действенную систему обеспечения безопасности, функционирование которой основывается на использовании подготовленных специалистов и эффективных (правда достаточно дорогостоящих) средств.

Во многом американская система может служить в качестве описательной модели при рассмотрении принципов и порядка ее функционирования. Система предполагает участие органов и сил всех уровней власти.

Руководство системой осуществляется с Национального центра защиты инфраструктуры, который отвечает за предупреждение, оповещение и реагирование на угрозы по отношению к КВИ. В рамках центра действует Координационный центр реагирования на угрозы в области информационных и компьютерных атак. Этот центр обеспечивает информационную безопасность путем непрерывного отслеживания обстановки и информационного трафика. В случае угрозы объектам информационной инфраструктуры изменяется характер деятельности на различных объектах.

К основным принципам функционирования системы относятся:

- открытость архитектуры;
- идентификация критически важных интерфейсов для подсистем и компонентов, в первую очередь тех, которые обладают наибольшей сложностью и стоимостью;
- использование общих стандартов, обеспечивающих последующую эволюционную модернизацию;
- использование модульности;
- минимизация затрат на создание, поддержание в функциональном виде и обслуживание;
- широкое использование критических и коммерческих технологий.

Система вводится в действие после проведения «доказанной пригодности» в виде успешного выполнения задач. Для работы широко используются базы данных, которые в сочетании с разработанными алгоритмами позволяют проводить автоматизированное планирование. Используемая с 2002 г. база данных по связям в террористических организациях TILAD (Terrorist Identification Linkage Analysis Database) позволяет в автоматизированном режиме выявлять опасные криминальные связи по банковским документам, сотовым соединениям и т. д. и повышать оперативность реа-

гирования. При обнаружении подозрительных сообщений система автоматически выдает сигнал предупреждения. Кроме того, она автоматически поддерживает взаимодействие между различными органами.

На каждом уровне управления развернуты свои органы на соответствующих пунктах управления, оснащенных средствами управления, связи и автоматизации.

В каждом штате при губернаторе создается **Центр защиты инфраструктуры.** При губернаторе штата действует Совет по защите КВИ, который по своему построению и функциям аналогичен с учетом масштабов и возможностей президентскому Совету по защите КВИ. Совет разрабатывает стратегию совершенствования системы обеспечения безопасности КВО и готовит практические и методологические предложения.

Центр защиты инфраструктуры замыкает на себя все связи с различными организациями различных ведомств и уровней.

Центр защиты КВИ выполняет следующие действия:

- разрабатывает подходы к распространению сети оповещения;
- обеспечивает работу закрытых систем связи, своевременность доведения информации;
- обеспечивает взаимодействие с органами управления всех уровней и правительственными ведомствами;
- определяет стандарты и процедуры взаимодействия для государственных органов и поставщиков;
- обеспечивает обучение и подготовку;
- включает систему судебного преследования за компьютерные преступления;
- разрабатывает государственный подход к восстановлению систем и нормальной жизнедеятельности.

Центр защиты КВИ выполняет функции обнаружения и оповещения об угрозах. Для этого он осуществляет:

- сбор информации;
- ее обзор и анализ;
- распространение информации об угрозах;
- нотификацию для слежения, предотвращения угроз;
- рекомендации губернатору, какую информацию следует обнародовать при наличии соответствующих рисков;
- контроль ситуации;
- архивирование информации для будущих обзоров в целях определения тенденций, проведения последующего анализа и создания прогнозных моделей.

Для сбора информации используются закрытые каналы связи, которые обеспечивают безопасность передачи секретной информации. Закрытие может производиться с помощью коммерческих методов. Информация от частного сектора и информационно-распределительного центра может не закрываться.

Обзор и анализ представляет собой критически важный момент работы для обнаружения и оповещения, он должен проводиться с учетом обеспечения требований своевременности, точности и надежности получаемой информации. Персонал может взаимодействовать посредством телефонных и электронных контактов для получения полной, ясной и проверенной информации с различными органами. Успех центра по предотвращению бедствия зависит от способности аналитиков провести анализ угроз и предвидеть их. В целях совершенствования системы защиты предполагается внедрить систему поддержки принятия решения — Homeland Security Advisory System, которая представляет собой унифицированную систему предупреждения об угрозах, эффективно распределяющую информацию о рисках по всем уровням власти, а также обеспечивающую ее доведение до населения. Система позволит оценивать, насколько угроза реалистична, подтверждается ли она различными источниками, каковы ее особенности, степень ее опасности и масштаб. Устанавливается пять степеней угроз:

1. Низкая («зеленый»).
2. Возможная («голубой»).
3. Возрастающая («желтый»).
4. Высокая («оранжевый»).
5. Очевидно высокая («красный»).

Каждой степени соответствует соответствующая совокупность мероприятий. Данная система позволяет оценивать, насколько вероятна угроза по пятибалльной системе.

Распространение информации Центром проводится с учетом установленных для потребителей приоритетов. При реальности возникающей угрозы требуется немедленное уведомление (нотификация) собственников КВО и операторов, обеспечивающих их эксплуатацию для использования возможности предотвратить ее или снизить последствия ее воздействия. Одновременно система позволяет проводить оповещение групп немедленного реагирования. Оперативность проведения уведомления в значительной степени зависит от типа возникающей угрозы (носит ли она физический или виртуальный характер, связана ли она с использованием химических, бактериологических средств). В значительной степени эффективность работы в данном случае зависит от степени подготовленности аналитиков центра.

Уведомление населения, общественных организаций и различных правительственных ведомств штата и затрагиваемых коммерческих ком-

паний проводится сразу же после оповещения фирм-владельцев КВО и групп немедленного реагирования. Штаб Центра готовится таким образом, чтобы распространяемые уведомления были бы максимально понятны и информативны. В данном случае всегда важной остается роль губернатора, который должен обеспечивать информирование населения об угрозах, в том числе лично через СМИ. Он определяет объемы и сроки доведения оповещений и информации до населения. Центр берет на себя ответственность за развитие ситуации при получении информации о возникающей угрозе и несет ее до прибытия специального штаба руководящего ведомства или вышестоящего органа, обеспечивая координацию действий на начальном этапе развития обстановки. Имеющаяся система управления и связи, развернутая на базе Центра, может использоваться во многих случаях и после прибытия сил вышестоящих звеньев управления. Кроме того, после передачи управления, персонал центра обязан контролировать обстановку, так как угроза может вылиться в серию согласованных или разрозненных нападений на КВО. Вся генерируемая информация в ходе операции должна архивироваться в базах данных для последующего анализа и передачи в вышестоящее звено, что позволит прогнозировать развитие ситуации в будущем. Секретная информация хранится, как правило, в базах частей Национальной гвардии, дислоцирующихся на территории штата.

Особое внимание уделяется сбору и анализу информации, циркулирующей в компьютерных сетях, так как она очень вероятно может использоваться для поддержания взаимодействия членами террористических групп (что отмечалось в 2001 г.) для получения информации о КВО, либо сама быть объектом атаки. Сами компьютерные сети, как глобальные, типа Интернет, так и местные и локальные, могут служить надежным и эффективным средством обмена данными и передачи информации для различных потребителей, в том числе с установленными заранее адресными группами, которые определяют списки определенных групп абонентов, которым она предназначается. Создание чатов в сети позволяет оперативно создавать сети для текущего обмена, в том числе с муниципальными органами, число которых может достигать нескольких сотен. Для обеспечения эффективной работы компьютерных средств и предотвращения атак на сети создаются специальные группы немедленного реагирования в области компьютерной безопасности.

Важное место в работе центра занимает взаимодействие с территориальными органами управления Национальной гвардии (НГ), которые имеют доступ к разведывательной и другой конфиденциальной информации. В некоторых случаях руководство НГ может выделять воинские контингенты для реагирования на обстановку и ликвидацию последствий катастроф.

В местном отделении ФБР имеется служба защиты инфраструктуры, которая взаимодействует с центром в ходе повседневной работы. Цель рабо-

ты службы заключается в информировании местных органов и владельцев объектов с тем, чтобы они могли обеспечить более надежную их защиту.

В ходе своей деятельности Центр защиты КВИ взаимодействует с такими органами как Национальный центр защиты КВИ, Национальным координационным центром обеспечения внутренней безопасности, ФБР, Региональным центром обмена информацией и другими органами.

Основная проблема в работе заключается в подготовке информации для анализа, до 85 % всего времени уходит на решение этой задачи. В решающей степени успех деятельности зависит от работы на местах и в районах кризисных ситуаций.

5. Оценка рисков нарушения безопасности КВО

Предметная область оценки рисков нарушения безопасности КВО показана на рис. 1.

Ключевым средством для создания эффективных систем защиты является интеграция технических систем и средств. Согласно известному принципу, говорящему, что прочность цепи определяется прочностью ее слабейшего звена, система безопасности должна рассматриваться в целом.

1. Критические важные объекты, уязвимость которых не определена или очень низкая
2. Уязвимость программ, населения, систем, оборудования, которые не характеризуются как КВО и не известны угрозы
3. Условия угроз, для которых не известны угрозы для КВО или доступ к слабым местам
4. КВО для которых известны уязвимости, но не известны угрозы
5. КВО для которых известны угрозы, но не известны уязвимости
6. Угрозы, требующие специальных знаний и/или возможности использовать слабые места, хотя нет уязвимости КВО

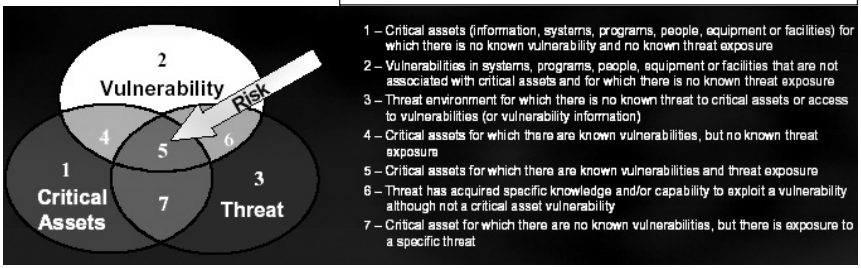

Рис. 1. Оценка рисков при защите КВО

Оценка рисков включает объединение информации, касающейся угроз, уязвимости объектов и возможных последствий. Управление рисками основывается на организации мер защиты на основе выработки стратегии снижения рисков. Многие модели и методологии выработаны с учетом использования имеющихся ресурсов на основе критерия «эффективность — стоимость». Большинство методологий включают в той или иной степени следующие элементы:

- определение важных объектов и выявление тех из них, которые могут считаться КВО;
- определение, описание и оценка угроз;
- оценка уязвимости КВО со стороны различных специфических классов угроз;
- определение риска (т. е. ожидаемые последствия специфических типов атак на специфические типы объектов);
- определение путей сокращения возникающих рисков;
- определение на основе выработанной стратегии приоритетов в выборе мер сокращения рисков.

Определение важных объектов и выявление тех из них, которые могут считаться критически важными

На этом этапе проводится описание важных объектов, которое включает характеристики зданий, транспортных средств, оборудования, средств хранения материальных запасов, средств контроля, складов, энергоблоков, средств водоснабжения, систем связи, информационных систем, оснащения офисов и т. д. Информация может содержать данные по продукции, описание производственного процесса, оперативные данные, бизнес-стратегию, финансовые данные, данные по сотрудникам и т. д. Считается, что не существует наиболее важной информации, те или иные данные могут иметь различную ценность в различных условиях обстановки. Однако и чрезмерное накопление информации и ее несистемность значительно затрудняют работу. Критичность определяется влиянием на потерю или приведение в непригодное состояние объекта. Наиболее важным считается влияние угроз на выживание населения, как работающего на предприятии и живущим вблизи объекта, так и нации в целом.

Последствия категорируются по различным направлениям и секторам:

- экономика;
- финансы;
- окружающая среда;
- здоровье и безопасность;

- технологическая среда;
- продолжительность воздействия.

При рассмотрении критической важности объектов учитывается не только масштаб эффекта нарушения его функциональности, но и такие факторы, как время на его восстановление, например нарушение работы важного объекта в течение короткого времени может иметь меньшие последствия в сравнении с остановкой на продолжительное время менее значимого объекта, кроме того средства на восстановление могут быть различными. Другим важным фактором является взаимное влияние одного объекта на другой, прекращение работы которого имеют большие последствия. В частности, вывод из строя объектов энергоснабжения приводит к прекращению работы телекоммуникационных средств или водоснабжения. Потеря связи к нарушению работы, управления и контроля других объектов, например автоматических аппаратов в банках и т. д.

Как правило, степень критичности объектов делится на три категории:

- высокая;
- средняя;
- низкая.

Кроме того, допускаются некоторые вариации этих категорий. Помимо этого применение различных методологий может привести к тому, что объект будет принадлежать к разным категориям. Например, методологии энергетического сектора подчеркивают высокую критичность происшествий, связанных с потерей крупных сумм денег, необходимостью созыва Совета директоров фирмы и простоем на продолжительное время, однако остановку производства на несколько дней не относят к таковым.

Кроме того, различные инстанции при совместном пользовании могут по разному оценивать критичность объекта, например, пользователь, эксплуатирующий систему, относит к первоочередным, а собственник нет. Наибольшую сложность представляют объекты, которые имеют сложный тип принадлежности и управления.

Определение, описание и оценка угроз

В ряде работ под угрозами принято понимать «признаки, обстоятельства или случаи, которые могут стать потенциальной причиной для потери или ущерба объекта».

Угрозы могут характеризоваться такими признаками как:

- тип угроз (инсайдер — внедренный или завербованный агент, террорист, военная угроза, стихийные бедствия — торнадо, ураганы);
- намерение и мотивация;
- порядок приведения в исполнение;

- возможности (подготовленность, специальные знания, доступ к необходимым материалам и оборудованию);
- методы (использование самоубийц, заминированных машин и другой техники, штурм, виртуальная атака);
- тенденции (какие способы и оснащение имели террористические группы и их опыт).

Информация об угрозах может поступать от разведывательных органов, органов правопорядка, специалистов, СМИ, результатов анализа и расследований произошедших инцидентов, из полученных угроз). Как правило, дополнительные затруднения вызывают: ложные звонки, взятие на себя ответственности непричастными лицами и организациями, скудность, фрагментарность и неопределенность имеющейся информации.

При оценке учитываются два фактора:

- представляет ли объект интерес для нападающих;
- имеет ли террористическая организация возможности для атаки каким либо способом.

При определении, описании и оценке угроз учитывается опыт террористических проявлений и составляются сценарии возможных действий. Экспертный совет Береговой охраны провел оценку эффективности 12 различных типов атак (например, катер со взрывчаткой подходит к танкеру на причале, танкер захвачен, или захваченное судно используется в качестве средства нападения) на 50 различных потенциальных объектов (например, топливозаправочный терминал), т. е. оценил 600 различных вариантов атак. Совет оценил вероятность каждого сценария, например использование военного корабля для доставки террористов оценено как маловероятное, а нападение на военный объект как очень вероятное. Каждому вероятному сценарию был присвоен один из пяти уровней вероятности появления после рассмотрения намерений и возможностей террористических групп, изучения опыта и имеющейся информации.

Методология, принятая в энергетическом секторе, использует перечень, который привязывается к специфическим характеристикам атак (использование взрывчатого вещества, транспортных средств, компьютерная атака) и насколько вероятно такая атака может быть проведена отдельными лицами или группой. После этого аналитик идентифицирует вероятность попадания объекта под сценарий и возможную цель нападения противника на объект. Как правило, оценка основывается на количественных параметрах, например вероятности совершения или качественно, например, «очень высокий уровень угроз». Полученные оценки не могут быть статичными во времени, степень угроз постоянно меняется во времени, в зависимости от таких факторов как развитие обстановки в том или ином районе, годовщины событий или необходимость напоминания о себе террористам.

Оценка уязвимости КВО со стороны различных специфических классов угроз

Уязвимость определяется как «слабость или слабое место, которые могут использоваться для получения необходимого доступа к заданному объекту». Слабые места могут характеризоваться по различным направлениям:

- физические (доступность, относительное местоположение, видимость, прочность, устойчивость и т. д.);
- технические (подверженность компьютерным атакам, устойчивость к перепадам энергоснабжения, загрязнение, землетрясение);
- оперативные (полиция, мероприятия по защите, порядок работы и привычки персонала);
- организационные (наличие и функциональность штабов и управленческих органов).

Оценка уязвимости призвана выявлять слабые места в условиях мер противодействия угрозам, детально оценивать их надежность и эффективность. Например, оценка уязвимости объекта при наличии сотрудников безопасности. Изучается сколько сотрудников обеспечивают дежурство, какими техническими средствами контроля они пользуются, патрулируют они или контролируют средства отображения обстановки, как они оснащены и тренированы, готовы ли они задержать или отразить нападающих при различных попытках проникновения, способны ли отразить различные попытки проникновения.

Уязвимость оценивается по отношению к конкретным типам атак. Национальная нефтехимическая и нефтеперерабатывающая ассоциация выделяет три этапа оценки уязвимости:

- определение того, как противник может проводить различные типы атак против специфичных объектов или групп объектов;
- оценка существующих мероприятий и контрдействий по их надежности и эффективности по предупреждению, сдерживанию, ограничению допуска, обнаружении и предотвращению атак;
- определение текущего состояния уязвимости и определение объемов проблем.

Береговая охрана оценивает уязвимость потенциальных целей нападения для каждого сценария атаки по четырем направлениям:

- привлекательность объекта для террористов (является целью или подвергался ли атаке подобный объект);
- доступность объекта (насколько легко противник может проникнуть или приблизиться к объекту);

- каковы штатные меры, силы и средства противодействия применяются (существующий план обеспечения безопасности объекта, возможности средств связи, системы обнаружения и предупреждения о проникновении, персонал службы безопасности);
- устойчивость объекта (характеристики его постройки и т. п., насколько сильное воздействие он может выдержать).

Каждое из этих четырех направлений оценивается по пятибалльной системе, каждый уровень соответствует определенной вероятности проведения успешной атаки. Для примера, уязвимость объектов энергоснабжения применительно к обеспечению из выживания в случае атаки оценивается на уровне 0,8.

Определение риска

Риск определяется как «вероятность потери или ущерба». В Береговой охране выделяют 6 основных категорий воздействия:

- уничтожение или повреждение;
- экономическое;
- ущерб окружающей среде;
- ущерб национальной обороне;
- символический;
- вторичные проблемы национальной безопасности.

Каждый сценарий оценивается по пятибалльной шкале от низкого уровня до катастрофы. Аналитики могут попытаться оценить риск качественно. Например, эксперты не знают, будет ли совершаться атака, следовательно, вероятность 0,5 (50/50), шанс использования конкретного типа атаки (например, с помощью начиненного взрывчаткой автомобиля) составляет 75/25 — вероятность 0,75, успех такой атаки оценивается как успешный 70/30, т. е. вероятность 0,3. Критерием успешной атаки может быть критерий гибели 500 человек и потери до 300 млн долл. Риск в данном случае оценивается следующим образом:

$$П_{общ} = (П_{люд} + П_{рес}) \times Р_а \times Р_т \times Р_у.$$

Здесь: $П_{общ}$ — общие потери,

$П_{люд}$ — потери людские,

$П_{рес}$ — потери ресурсов,

$Р_а$ — вероятность того, что атака будет совершена,

$Р_т$ — вероятность того, что атака будет определенного типа,

$Р_у$ — вероятность того, что атака будет успешной.

Таким образом, общая оценка составит 56 человек и 33,8 млн долл.

Достаточно часто используются чисто качественные оценки, например — высокий уровень, средний, низкий. Общая оценка может быть многовекторной.

Определение путей сокращения возникающих рисков

Риски могут быть снижены различными путями:

- снижением уровня угроз (например, путем перехвата или уничтожения противника до нанесения удара);
- снижением уязвимости (повышением устойчивости объектов по отношению к атакам);
- сокращением влияния неблагоприятных последствий атак (защита населения и т. д.).

Каждое из отдельных мероприятий повышает общий системный эффект. Каждое мероприятие оценивается, при этом стоимость может многомерной. Это могут быть прямые финансовые потери, затраты на материалы, оснащение, оборудование и подготовку. На долгосрочную перспективу это затраты на обслуживание и ремонт, оплата персонала.

Определение на основе выработанной стратегии приоритетов в выборе мер сокращения рисков

Большинство методов основывается на использовании критерия «эффективность — стоимость».

В качестве ведущего органа, обеспечивающего проведение оценок рисков, определен департамент информационного анализа и защиты инфраструктуры МВБ США. Департаментом составлен список КВО, который включает более 33 тыс. объектов. Из этого списка выделены 1 700, которые рассматриваются в качестве критически важных с точки зрения национального масштаба. Для каждого из этих объектов департамент провел необходимые оценки рисков. Полученные оценки положены в основу приоритетных работ по защите критически важной инфраструктуры в виде планов и организации взаимодействия с другими ведомствами, в первую очередь разведывательными.

В соответствии с Законом о внутренней безопасности 2002 г. оценки рисков производятся следующим образом:

- выявляется и оценивается природа и масштаб террористических угроз для внутренней безопасности;
- анализируются угрозы с точки зрения фактической и потенциальной уязвимости системы внутренней безопасности;
- проводится оценка уязвимости ключевых ресурсных систем и критически важной инфраструктуры США, включая оценку рисков для оп-

ределения возможностей атак, проводимых с территории континентальной части США;

- обобщение всей относящейся к проблеме информации, проведение анализа, оценки уязвимости для определения приоритетов мер защиты и обеспечения восстановления жизнедеятельности объектов;
- разработка всеобъемлющего плана обеспечения безопасности ключевых объектов.

Разрабатываемые в МВБ планы и методологии призваны обеспечить работу в чрезвычайных условиях различных руководящих и других органов, в том числе федеральных, органов власти штатов и местных органов, а также неправительственных организаций и фирм. В ряде государств большая часть КВО находится в собственности не государства, а различных фирм и корпораций (например, в Великобритании доля таких объектов достигает 70 %).

В настоящее время предполагается, что доля рисков, связанных с террористической деятельностью, становится преобладающей в сравнении с традиционными угрозами.

Многие государственные и негосударственные организации выработали собственные методологические документы, обеспечивающие противодействие угрозам. Министерство энергетики опубликовало «Перечень мероприятий по управлению рисками в области энергоснабжения применительно к мелким и средним объектам». Американский Совет химической промышленности выпустил «Руководство по безопасности объектов химической промышленности». Национальная нефтехимическая и нефтеперерабатывающая ассоциация разработала «Методологию оценки уязвимости и нарушения безопасности нефтяной и химической промышленности».

Список использованных источников

Ниже приводится перечень директивных документов, регламентирующих деятельность органов государственного управления различных уровней по обеспечению безопасности КВО, опубликованных в открытой печати, на основании которых составлен настоящий обзор.

1. Закон о стихийных бедствиях (P.L. 93-288) от 22 мая 1974 г.
2. Закон Стаффорда о стихийных бедствиях и чрезвычайных службах (P.L. 93-288) от 23 ноября 1988 г.
3. Федеральный закон о реформе в области информационной безопасности (GISRA — Government Information Security Reform Act), 2000 г.
4. Оперативный план взаимодействия правительственных ведомств при борьбе с терроризмом (CONPLAN), директивы президента США № 39 и 62, январь 2001 г.

5. Директива Президента США № 63 о критически важной инфраструктуре и развертывании Национального центра защиты инфраструктуры (NIPC — National Infrastructure Protection Center) от 22 мая 1998 г.
6. Национальная стратегия внутренней безопасности, июль 2002 г.
7. Закон о внутренней безопасности (P.L. 107-296) от 25 ноября 2002 г.
8. Определение критически важной инфраструктуры, приоритеты и защита. Директива Президента США по внутренней безопасности № 7 от 17 декабря 2003 г.
9. Указ Президента США 13010 от 15 июля 1996 г. об учреждении комиссии по защите критически важной инфраструктуры при президенте.
10. Указ Президента США 13228 от 8 октября 2001 г. о централизации системы национальной и внутренней безопасности.
11. Указ Президента США 13231 от 16 октября 2001 г. о Совете по защите КВИ.
12. Директива Президента США № 39 от 21 июня 1995 г. по контртерроризму и мерах по обеспечению продовольственной безопасности.
13. Директива Президента США № 62 от 22 мая 1998 г.по терроризму и защите критически важных объектов инфраструктуры.
14. Директива Президента США № 5 от 28 февраля 2003 г. по внутренней безопасности МВБ.
15. Закон о морской транспортной безопасности (P.L. 107-295) от 25 ноября 2002 г.
16. Закон о береговой охране и морском транспорте (P.L. 108-293) от 9 августа 2004 г.
17. Закон о безопасности в области здравоохранения, готовности к биотерроризму и реагировании на него (P.L. 107-188) от 2002 г.
18. Директива МО США 3025.15 об операциях по поддержке гражданских органов управления и помощи населению внутри страны от 1 июля 1993 г.

Приложение

Терроризм в Интернете

Авторы обзора сочли целесообразным дополнить его результатами исследования, выполненного Габриелем Вайманном, профессором теории коммуникации из Университета Хайфы, посвященного методам использования террористами Интернета. Эти результаты, представленные в *YaleGlobal Online* от 26 апреля 2004 г., приведены ниже. Текст с небольшими сокращениями цитируется по русскому переводу книги Томаса Фридмана «Плоский мир» (М.: Изд-во АСТ, 2006. С. 553).

Несмотря на то, что угроза кибертерроризма для Интернета сегодня часто становится предметом публичных дискуссий, на удивление мало людей знают о том, какую угрозу на самом деле представляет использование террори-

стами самого Интернета. Ведущееся на протяжении последних шести лет исследование показывает, что террористические организации и их сторонники пользуются всеми доступными интернет-средствами для вербовки новых членов, сбора денежных пожертвований и проведения глобальных кампаний устрашения. Можно также сделать вывод, что для эффективной борьбы с террористами недостаточно выявлять и закрывать их сетевые ресурсы. Наш всесторонний анализ Интернета в 2003–2004 гг. выявил существование сотен вебсайтов, которые обслуживают террористов самыми разнообразными, хотя и часто пересекающимися способами. Террористы используют это неподцензурное виртуальное пространство для запуска дезинформации, для обнародования угроз, призванных вселить в людей чувство беспомощности, для распространения фото- и видеоматериалов о своих последних «акциях».

После 11 сентября 2001 г. «Аль-Каида» разместила на своих сайтах целую серию предупреждений о грядущей «большой атаке» на объекты в Соединенных Штатах. Эти «анонсы» получили широкое освещение в СМИ, что способствовало нагнетанию настроений страха и незащищенности по всему миру, и особенно в США.. Интернет значительно расширил доступ террористов к общественному восприятию. До возникновения Интернета расчет террористов на то, что их позиция и деятельность сумеют получить огласку, во многом зависел от привлечения внимания телевидения, радио и печати. То обстоятельство, что теперь террористы способны напрямую контролировать содержание своих сайтов, дает им в руки дополнительные возможности формировать восприятие различных целевых аудиторий, манипулировать как своим образом, так и образом своих врагов, перед лицом общественности. Как правило, сайты террористических организаций не сосредотачиваются на актах насилия. Вне зависимости от их сущности, мотивов или местоположения большинство из них акцентируют внимание на двух вопросах: ограничениях свободы слова и печальной участи своих соратников-политзаключенных. Эти темы находят огромный резонанс у их собственных сторонников и также рассчитаны на привлечение симпатий граждан западных стран, которые дорожат правом на свободу высказывания и неодобрительно относятся к попыткам преследования политической оппозиции.

Террористы показали себя не только мастерами онлайнового маркетинга, но и высококлассными экспертами по извлечению нужных данных из недр Всемирной паутины, насчитывающей сегодня миллиард с лишним страниц. Через Интернет они способны узнавать расписание работы и местоположение будущих мишеней: транспортных средств, атомных электростанций, публичных зданий, воздушных и морских портов, они способны даже почерпнуть информацию о принятых контртеррористических мерах. По сообщению министра обороны США Дональда Рамсфельда, в одной из инструкций «Аль-Каиды», обнаруженных в Афганистане, говорилось, что «благодаря открытому и абсолютно законному использованию общедоступных ресурсов можно

собрать как минимум 80 % необходимой информации о противнике». В одном захваченном компьютере, принадлежавшем «Аль-Каиде», содержалась инженерная и архитектурная схема плотины, которая была скачана из Интернета и позволяла инженерам и стратегам организации разыгрывать с ее помощью самые разные катастрофические сценарии. В других захваченных компьютерах сотрудники спецслужб США обнаружили доказательства того, что операторы «Аль-Каиды» проводили немало времени на сайтах, содержащих информацию о программном обеспечении систем транспорта, связи, энерго- и водоснабжения и инструкции по их компьютерному управлению.

Как и другие политические организации, террористические группы эксплуатируют Интернет для сбора средств. К примеру, «Аль-Каида», всегда зависевшая от внешних пожертвований, связана с целой глобальной сетью, которая опирается на благотворительные учреждения, неправительственные организации, другие финансовые институты, использующие для своих целей веб-сайты и виртуальные форумы. Вооруженные повстанцы в российской Чечне обнародовали в Интернете номера банковских счетов, куда сочувствующие могли переводить им средства. В декабре 2001 г. американское правительство наложило арест на активы одной из техасских благотворительных организаций, которая, как выяснилось, была связана с «Хамасом».

Кроме размещения на веб-сайтах просьб о финансовой помощи, террористы используют в качестве средств убеждения и вербовки новичков самый широкий спектр веб-технологий (цифровое видео, аудио и пр.). И подобно администраторам коммерческих ресурсов, они тоже ведут учет людей, которые заходят на их сайт. С теми, кто попадает в разряд интересующихся или кто кажется им подходящей кандидатурой для выполнения поручений, террористические организации входят в контакт. Вербовщики могут использовать и более интерактивные веб-технологии, заходя в чаты и киберкафе и подыскивая среди участников, особенно молодых, тех, кто наиболее восприимчив к их пропаганде. Институт СИТЕ — вашингтонская группа исследователей терроризма, которая занимается мониторингом интернет-коммуникаций «Аль-Каиды», — обнародовал шокирующие подробности высокотехнологической вербовочной кампании 2003 г., целью которой был призыв боевиков, подлежащих заброске в Ирак для борьбы с силами антитеррористической коалиции. В довершение, Интернет обеспечивает террористам дешевое и надежное средство налаживания и поддержания контактов. Многие террористические группировки, в том числе «Аль-Каида» и «Хамас», за последнее время трансформировались из строго иерархических организаций с назначаемыми руководителями в объединения полунезависимых ячеек, которые не имеют единого центра власти. Через Интернет члены этих частично разобщенных групп способны общаться между собой и налаживать связи с представителями других аналогичных сообществ. Десятки сайтов, поддерживающих террористическую тактику джихада, позволяют жителям таких удаленных друг

от друга регионов, как Чечня и Малайзия, обмениваться не только идеями, но и практической информацией по изготовлению бомб, организации новых ячеек, осуществлению акций. Во время планирования и координации захвата самолетов 11 сентября члены «Аль-Каиды» во многом полагались именно на Интернет.

Томас Фридман комментирует сказанное следующим образом:

Все это говорит о том, что мы только начинаем понимать геополитические последствия глобального развития Интернета… Нет ничего опаснее в современном мире, чем обанкротившаяся страна с широкополосным доступом в Интернет. Другими словами, сейчас даже в самых отсталых государствах, как правило, есть телекоммуникационные системы и спутниковые антенны. Следовательно, если в таком государстве найдет себе приют террористическая сеть (как это случилось с «Аль-Каидой» в Афганистане), его могущество способно увеличиться до невероятных масштабов. Как бы ни хотели мировые державы держаться подальше от неблагополучных регионов, они иногда чувствуют себя вынужденными все глубже ввязываться в их проблемы. Вспомните об Америке в Афганистане и Ираке, о России в Чечне, об Австралии в Восточном Тиморе.

Хотя в плоском мире становится все сложнее спрятаться, в нем гораздо проще оставаться на связи. «Возьмите Мао в начале китайской коммунистической революции, — заметил Майкл Мандельбаум, специалист по внешнеполитическим вопросам из Университета Джонса Хопкинса. — Китайским коммунистам приходилось скрываться в пещерах на северо-западе страны, но когда они захватывали какую-либо территорию, они могли спокойно по ней передвигаться. Бен Ладен, наоборот, не высовывает носа, но благодаря Интернету способен дотянуться до каждого дома на планете». Бен Ладен не может завладеть никакой территорией, зато может спокойно овладевать воображением миллионов. Он уже проделал это — объявившись на экранах телевизоров в американских гостиных накануне президентских выборов 2004 г.

Не так страшен черт, как террорист со спутниковой тарелкой и интерактивным веб-сайтом.