

Стр. 3-4

Энергетическая
безопасность:

- Юргита Билваисиене – Литва,
- Дитер Урбан – председатель Комитета промышленного планирования НАТО

Стр. 5-6

Киберзащита:

- Лигия Феррейра – председатель Комитета по планированию гражданской связи НАТО
- Сулейман Анил – руководитель Центра координации и поддержки по киберзащите НАТО

Стр. 8

Пиратство:

- Джим Капонити – председатель Совета по планированию морского судоходства НАТО

Стр. 9

Пандемии:

- Эрик Лекарпентье – председатель Объединенного медицинского комитета НАТО

Стр. 12

- Научная программа НАТО по киберзащите в странах-партнерах – Джейни Клинтон

Стр. 13

- Мероприятия в СКЕПСИ

Стр. 14-15

- EADRCC Update: Новости ЕКЦРСБК: «ЭйдМатрикс» - Гюнтер Бретшнайдер, руководитель ЕКЦРСБК

Отказ от ответственности: Данный бюллетень публикуется под эгидой помощника Генерального секретаря НАТО по операциям. Взгляды, выражаемые в данной публикации, не обязательно отражают официальное мнение или политику правительств стран-участниц НАТО или самой организации.

ОТ РЕДАКЦИИ

Мартин Ховард, помощник Генерального секретаря НАТО по операциям



ГРАЖДАНСКОЕ ЧРЕЗВЫЧАЙНОЕ ПЛАНИРОВАНИЕ – НОВЫЕ РИСКИ И ВЫЗОВЫ

В отличие от прошлого, сейчас обеспечение безопасности ориентировано почти исключительно на защиту людей, а не территорий. Новые угрозы и вызовы, о которых повествуется в данном номере, достаточно наглядно иллюстрируют тот тезис. Энергетическая безопасность, киберзащита, пиратство и пандемии выходят за пределы национальных границ и ставят под угрозу не национальные границы, а население.

В данном номере поднимается ряд вопросов. Достаточно ли работы осуществляется на уровне гражданского чрезвычайного планирования? Может ли ГЧП активнее привлекаться к другим областям деятельности? Соответствуют ли этим задачам багаж технических знаний, которым владеет резерв гражданских экспертов ГЧП? Тема, не охваченная в этом номере, - глобальное потепление и его способность обострять риски национальной стабильности. Должно ли ГЧП подумать о расширении своего экспертного охвата и приложить больше усилий к смягчению последствий глобального потепления, в том числе, чаще задействуя Евроатлантический координационный центр реагирования на стихийные бедствия и катастрофы?

Недавно в своей речи, посвященной началу работы над новой Стратегической концепцией, Генеральный секретарь НАТО заявил, что дискуссия должна основываться не на том, что НАТО может делать, а на том, что ей следует делать; не на том, как адаптировать миссии к имеющимся в наличии силам и средствам, а на том, как адаптировать силы и средства к преодолению стоящих перед нами вызовов. Все это применимо и к гражданскому чрезвычайному планированию. Слишком часто мы сосредоточиваемся на том, как «продать» существующие продукты, а именно, уже имеющиеся экспертные знания. Возможно, нам следует уделять больше внимания тому, как адаптироваться к меняющейся обстановке и создавать инновационные продукты, думая о будущем. Мы постоянно слышим, что к вызовам безопасности в XXI веке невозможно подходить с менталитетом XX-го. Источник силы НАТО заключается в присущей ей двухвекторности, как военно-гражданскому союзу. Преодоление новых вызовов станет эффективнее, если совместное военно-гражданское планирование и операции станут нормой.

Вопрос заключается в том, как установить необходимое равновесие. НАТО, как организация, должна несомненно решать наиболее насущные текущие и будущие задачи обеспечения безопасности, но ей следует избегать опасности распыления своих сил на многих направлениях. Предстоящая дискуссия о новой Стратегической концепции, рассчитанная на несколько месяцев, поможет выявить данные приоритеты и найти точки равновесия.

ЦИТАТА ДНЯ

Помимо самых легко распознаваемых угроз, за последнее десятилетие появился целый ряд вызовов, которые все сильнее и сильнее сказываются на безопасности. Говоря об этих вызовах, я имею в виду энергетическую безопасность или защиту от кибератак и наше осознание возрастающего влияния глобального потепления на стабильность государств и международное использование ценных ресурсов, таких как вода.

Яап де Хооп Схеффер, Генеральный секретарь НАТО, на открытии семинара о новой стратегической концепции, 7 июля 2009 г.

Работая над преодолением новых вызовов и угроз, ГЧП играет опорную роль, благодаря своему активному и комплексному подходу к партнерству. Уже давно страны-партнеры могут принимать участие в дискуссиях о претворении в жизнь политики НАТО в духе открытости и солидарности. Помимо этого, у многих партнеров имеется существенный опыт в специфических областях, и НАТО может многому у них поучиться.

Чтобы избежать дублирования усилий при преодолении новых угроз, жизненно важно также сотрудничать с международными организациями. Например, над многими из охваченных в данном номере новых угроз также работает Евросоюз. Часто граница между мандатами обеих организаций едва ощутима.

В заключение следует сказать, что ни одна из стран не застрахована от глобальных угроз, и всегда существует потребность в сотрудничестве для противодействия общим вызовам. Деятельность НАТО в области гражданского чрезвычайного планирования позволяет самым действенным образом обмениваться информацией и передовыми наработками. ГЧП уже занимается решением данных задач и готово одним из первых вооружиться для этого новым менталитетом. Несомненно, многое еще можно предпринять, чтобы полнее задействовать потенциал ГЧП в области совместного военно-гражданского планирования и поддержки операций, в частности, существующие связи с партнерами для использования их экспертных знаний в конкретных областях. Ясно одно, - наибольшая ценность ГЧП заключается в огромных возможностях наращивания контактов благодаря целому ряду сопряжений с гражданскими ведомствами в самых разных областях, начиная с планирования промышленного производства и заканчивая медицинской проблематикой. Это обеспечивает превосходный фундамент для создания структур, способных эффективно защищать население и локализовывать воздействие кризисов.



ЗНАЕТЕ ЛИ ВЫ, ЧТО...

До настоящего времени 28 стран подписали Меморандум о понимании об облегчении жизненно важных трансграничных перевозок, а именно: Австрия, Албания, Армения, Болгария, Босния-Герцеговина, бывшая Югославская Республика Македония*, Великобритания, Венгрия, Германия, Грузия, Дания, Испания, Канада, Литва, Молдова, Нидерланды, Норвегия, Польша, Португалия, Словакия, Словения, США, Турция, Украина, Финляндия, Хорватия, Швеция и Эстония. Данный меморандум сокращает сроки и повышает эффективность оказания помощи жертвам гуманитарных кризисов, стихийных бедствий и катастроф, в том числе в ситуациях, вызванных химическим, биологическим, радиологическим или ядерным (ХБРЯ) инцидентом, в пределах региона СЕАП.

* Турция признает Республику Македонию под ее конституционным названием.

Фото: Меморандум подписывают США (посол Иво Даалдер), Польша (посол Богустав Винид) и Эстония



Автор первой статьи в этом разделе – представитель Литвы, члена НАТО, имеющего экспертные знания и приоритеты в области энергетической безопасности. Автор второй - Дитер Урбан, председатель Комитета промышленного планирования НАТО. Его статья посвящена мероприятиям в области защиты энергетической инфраструктуры – одному из основных направлений работы этого комитета.

Подход Литвы к вопросу энергетической безопасности

Энергетическая безопасность является неотъемлемым компонентом эффективной экономики и ключевым элементом национальной безопасности и гражданской защиты. Надежные поставки энергоресурсов из разнообразных источников, наряду с их устойчивым, эффективным потреблением в немалой степени определяют благосостояние отдельно взятого государства. Следовательно, энергетическая безопасность способствует стабильности международного сообщества в целом. В последние годы стало понятно, что характер проблем энергетической безопасности не просто национальный или региональный, и что насущной необходимостью является поиск глобальных решений.

Вопрос энергетической безопасности вошел в повестку дня НАТО сравнительно недавно. Учитывая, что перебои в потоках энергоресурсов могут затрагивать безопасность членов Североатлантического союза, мы считаем, что НАТО, как военно-политическая организация, должна также взять на себя выполнение задач в сфере энергетической безопасности. Ни у какой из существующих международных организаций нет монополии в данном вопросе. Поэтому роль НАТО не должна сводиться только к защите энергетической инфраструктуры. Эта задача важна, но кроме нее есть и другие, не менее важные составляющие. Нельзя забывать и о политическом компоненте энергетической безопасности. Нам требуется последовательный и сбалансированный подход с учетом технической и политической составляющих.

Для Литвы вопрос энергетической безопасности всегда имел особое значение. В силу своей истории Литва находилась в изоляции от стран Евросоюза и НАТО в том, что касается энергетического сектора. Помимо этого, страна всецело зависит от поставок российского газа и в большой степени – от экспорта российской нефти. Ситуация может еще более осложниться после закрытия Игналинской АЭС, которая удовлетворяет большую часть текущих потребностей страны в электроэнергии. Поэтому нашей основной целью в обозримом будущем является интеграция литовской энергетики в общий энергетический рынок Евросоюза и снижение нашей зависимости от единственного внешнего поставщика.

Наша зависимость от единственного поставщика энергоносителей считается одним из важнейших вопросов безопасности, следовательно, стратегическое значение приобретает диверсификация источников поставок энергоресурсов. Чтобы достичь этой цели нам требуется активизировать диалог между энергетическими компаниями, потребителями и транзитными странами. Диалог этот должен строиться на принципах транспарентности, недискриминации, взаимного доверия, взаимности и свободного доступа к транзитным маршрутам, сформулированных в Договоре к Энергетической хартии. НАТО может стать связующим звеном между странами, чьими силами будет действовать механизм сотрудничества в энергетическом секторе.

Следует отметить, что диверсификация поставок энергоресурсов – лишь одна сторона проблемы. Нам также требуется диверсифицировать и структуру энергетики. В условиях сокращения запасов традиционных энергоносителей и колеблющихся цен, рост энергопотребления отрицательно сказывается на климате нашей планеты. Глобальное потепление сегодня является одной из проблем планетарного масштаба, которую можно решить, главным образом, с помощью двух мер: а) более эффективного использования запасов энергоресурсов и б) роста потребления возобновляемой энергии и энергоносителей, не усугубляющих парникового эффекта, в том числе, ядерной энергии.





Безопасность поставок жизненно важных ресурсов непосредственно увязана с безопасностью населения стран НАТО, обеспечение которой является одной из основных обязанностей гражданского чрезвычайного планирования НАТО (ГЧП). Усилия ГЧП в этой сфере могут быть сосредоточены, главным образом, над решением технических вопросов на глобальных форумах. В недалеком будущем министерство иностранных дел Литвы совместно с Комитетом промышленного планирования НАТО и Комитетом программы «Наука ради мира и безопасности» планируют осуществлять совместные проекты по энергетической безопасности для содействия диалогу в энергетическом секторе и защиты объектов жизнеобеспечения.

В заключение можно сказать, что только совместные усилия, дальновидность и стратегический подход к энергетической безопасности позволят нам выработать непревзойденный образ мышления, на основе которого можно будет преодолевать самые серьезные вызовы в будущем.

РАБОТА КОМИТЕТА ПРОМЫШЛЕННОГО ПЛАНИРОВАНИЯ НАТО В ОБЛАСТИ ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ



В свете стоящих перед Североатлантическим союзом новых вызовов и выполняемой НАТО работы в области энергетической безопасности, Комитет промышленного планирования (КПП) под руководством Главного комитета гражданского чрезвычайного планирования с июня 2004 г. занимается смежными вопросами ГЧП. С самого начала сформировалось общее политическое понимание того, что КПП следует заниматься исключительно физическими аспектами защиты энергетической инфраструктуры. Вопросы безопасности жизненно важных энергоресурсов и их поставок в КПП не анализируются. Деятельность КПП сосредоточена на мониторинге угроз безопасности, в особенности терроризма, что входит в обязанности правительств стран или требует координации усилий правительств и частного сектора.

Приоритетом КПП является защита электроэнергетической инфраструктуры, так как это оказывает непосредственное воздействие на большинство отраслей промышленности и основные функции общества. В этой связи анализу подверглись нефтяная и газовая инфраструктура.

Системы энергообеспечения выходят за пределы государственных границ, и поэтому столь важным является сотрудничество между государствами-членами НАТО, особенно со странами-партнерами. По этим соображениям КПП привлекает государства-члены Совета евроатлантического партнерства (СЕАП) к тесному сотрудничеству в рамках работы по энергетической безопасности. Комитет анализирует энергетическую инфраструктуру в пределах территории стран НАТО/СЕАП и, в частности, уделяет особое внимание пунктам пересечения границ. Поскольку владельцами энергетической инфраструктуры часто являются частные операторы, в анализе КПП важное место отводится государственно-частному партнерству.

В своей работе КПП стремится разъяснять планировщикам на уровне правительства, насколько важно обмениваться информацией, а также укреплять диалог и развивать двусторонние контакты между национальными представителями при КПП, промышленными экспертами и среди других комитетов НАТО, занимающимися объектами энергетической инфраструктуры.

На семинарах и пленарных заседаниях комитета при содействии промышленных экспертов, специализирующихся на энергетике, обсуждаются защитные меры, происходит обмен опытом, распространяется информация о происходящем на рынках энергоресурсов. Ввиду различия в системах защиты, КПП считает более целесообразной разработку политики обмена передовыми наработками, чем составление перечня защитных мер. Разрабатываемая в КПП политика не носит обязательного характера. Передовые наработки призваны способствовать обмену информацией, обеспечивать рекомендации общего характера и направлять информацию правительственным органам, нуждающимся в руководящих указаниях и отвечающим за защиту энергетической инфраструктуры.

В результате появились передовые наработки для защиты сетей газо- и электроснабжения. Сейчас идет работа над каталогом передовых наработок по защите нефтяной инфраструктуры. Данную политику могут взять на вооружение соответствующие органы, чтобы обеспечить внедрение передовых наработок и принятие операторами надлежащих мер по защите инфраструктуры.

Произошедшие весной 2007 г. в Эстонии кибератаки против государственных Интернет-сайтов напомнили о том, сколь уязвимы ключевые системы перед враждебным действиям в современном открытом обществе. Лигия Феррейра, председатель Комитета по планированию гражданской связи НАТО, рассказывает о рисках и вызовах, которые таит в себе взаимосвязанное информационное общество. Сулейман Анил, руководитель Центра координации и поддержки по киберзащите НАТО, раскрывает принимаемые НАТО меры по защите своих информационно-коммуникационных систем от попыток нарушить их функционирование посредством кибератак.

РИСКИ И ВЫЗОВЫ ВО ВЗАИМОСВЯЗАННОМ ОБЩЕСТВЕ



Опорой современного информационного общества являются электронные коммуникационные сети. Благодаря этим взаимосвязанным сложным «распределенным системам» произошел резкий рост во всех секторах, использующих компьютеры, инфраструктуру, электронные услуги и приложения, известных под общим названием информационно-коммуникационных технологий (ИКТ). Естественно, для круглосуточной эксплуатации данных систем в глобальном масштабе необходимо наличие соответствующей взаимосвязанной и взаимозависимой инфраструктуры. Все эти факторы создают крайне сложную и рискованную обстановку, с которой приходится иметь дело государствам. К счастью, у НАТО имеется ряд структур и механизмов для разрешения многих возникающих в этой связи проблем. Одним из ключевых органов, занимающихся такой деятельностью, является Комитет по планированию гражданской связи (КПГС).

КПГС существует свыше 50 лет, и ему поручено предоставление консультаций государствам НАТО и СЕАП по всем аспектам готовности к гражданским чрезвычайным ситуациям, имеющим отношение к гражданской связи. Комитет отвечает за разработку и координацию механизмов, необходимых для обеспечения функционирования гражданской связи во время кризиса, насколько это представляется осуществимым. Это включает, в частности, разработку и предоставление государствам рекомендаций о новых и перспективных технологиях, в том числе по кибербезопасности и киберзащите.

Киберзащита, которая подразумевает защиту информации путем предотвращения кибератак, их детекции и принятия ответных мер, должна обеспечиваться на всех уровнях. Правительствам необходимо засекретить свои электронные информационные сети и системы для защиты всей государственной деятельности, а именно обороны, логистики, транспортных и финансовых систем, инфраструктуры и личных данных граждан. Особую тревогу государств вызывает тот факт, что кибератака одной правительственной системы или сектора вполне может иметь серьезные последствия для других таких систем.

Организаторами кибератак могут быть частные лица, преступные элементы, авантюристы, или их могут финансировать правительства враждебно настроенных стран или транснациональные организации. Их способности, мотивация и готовность воспользоваться уязвимыми местами, видимо, не имеют границ. Помимо этого, в случае изоциренных кибератак практически невозможно отыскать их подлинный источник. Такая анонимность, в которой действуют сегодняшние авторы кибератак, создают существенные трудности у пострадавших государств, старающихся принять ответные меры.

Результаты таких кибератак, совершенных во время стихийного бедствия, техногенной катастрофы или другого кризиса, например, теракта, могут иметь катастрофические последствия для жизнеспособности государства. Они способны серьезно нарушить повседневный информационный поток между различными правительственными министерствами или ведомствами, преградить доступ к информации пострадавшему населению. Они также могут помешать аварийно-спасательным службам оказать своевременную помощь в пострадавшем районе. Наконец, они могут лишить страну возможности сотрудничать с соседними странами или на уровне региона при реагировании на международный кризис или стихийное бедствие.



КПГС непосредственно занимается вопросами кибербезопасности с 2003 г. В соответствии с его текущей Рабочей программой, комитет проводит оценку существующих на национальном уровне и потенциально уязвимых мест электронных коммуникационных сетей перед кибератаками. Исследуются также и другие угрозы, такие как пассивная утечка информации из электронных компонентов или систем. По запросу государств КПГС ранее анализировал другие вопросы кибербезопасности, такие как последствия кибератак, защита информационных сетей и возможность использования схем приоритизации для предотвращения перегрузки или аварий на системах.

Дополнительной опорой комитета служит группа экспертов по киберзащите, базирующихся в странах-членах, но готовых выполнять задачи по запросу организации на основе Договоренностей по гражданскому чрезвычайному планированию для управления в кризисных ситуациях. Запросы о поддержке и предоставлении рекомендаций могут поступать в НАТО от стран СЕАП, участников программы «Средиземноморский

диалог» и Стамбульской инициативы сотрудничества, а также от военных структур Североатлантического союза. Страны обращаются за такой поддержкой в случае реальных кризисных ситуаций или с целью оценки потребностей во внедрении программ киберзащиты. Вышеупомянутые эксперты также готовы оказать содействие другим органам НАТО, ведающим кибербезопасностью, например, Центру НАТО по реагированию на компьютерные инциденты (см. статью г-на Анила), Совету НАТО по ККУ и другим структурам.

Конечно, КПГС не может выполнять свои задачи в отрыве от других структур или организаций. В состав членов комитета входят старшие должностные лица из национальных министерств связи, многие из которых также являются национальными представителями по ИКТ в международных организациях, таких как Международный союз электросвязи ООН и Евросоюз. Следовательно, между организациями существует налаженный обмен информацией без излишних формальностей, что позволяет избегать дублирования усилий.

Сегодняшнее взаимосвязанное информационное общество отражает текущие потребности и указывает на будущие тенденции. Зависимость частных лиц, государств и международных организаций от электронных услуг, инфраструктуры и приложений будет безусловно усиливаться, равно как и соответствующие потребности в более усовершенствованной кибербезопасности. Государства-члены Североатлантического союза четко сформулировали роль НАТО в данной области, и Комитет по планированию гражданской связи будет продолжать выполнять свои обязанности, как звено общей системы.

ЗАЩИТА ОТ КИБЕРАТАК



Первые сообщения о случаях кибератак против информационных систем НАТО начали поступать в конце 1990-х гг. во время операций НАТО на Балканах. В результате некоторых из этих атак произошел взлом информационно-коммуникационных систем НАТО, что вызвало перебои в эксплуатационном обслуживании НАТО. Основываясь на опыте операций на Балканах, на Рижской встрече в верхах НАТО в 2002 г. правительства стран-участниц призвали «усовершенствовать защиту ключевых информационных систем от кибератак». На основе данной декларации был принят ряд внутренних мер, чтобы усилить позиции организации в плане кибербезопасности. Наиболее значительной и комплексной инициативой явился начатый в 2003 г. проект создания Центра реагирования на компьютерные инциденты НАТО. Центр действует с конца 2005 г. и отвечает на сообщаемые инциденты в системе безопасности на сетях НАТО.

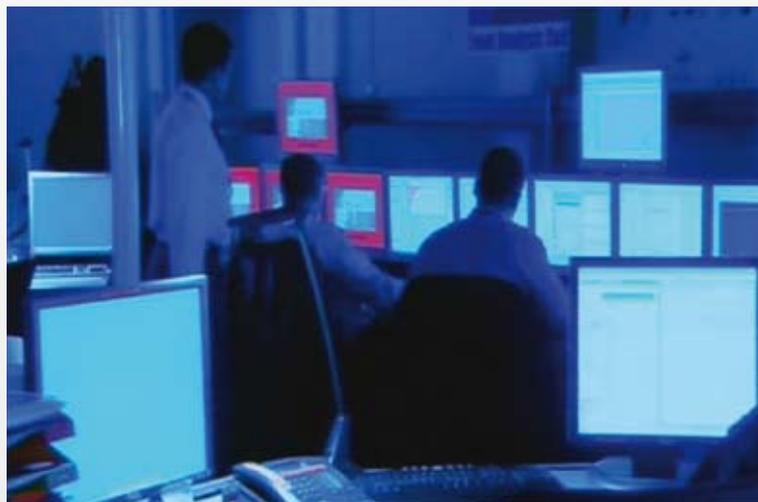
В мае 2007 г. весь мир стал свидетелем того, как член НАТО Эстония пала жертвой кибератак, направленных против ее ИТ-инфраструктур и онлайн-услуг в результате политического конфликта. Эти нападения – первые в своем роде – продлились около трех недель, наглядно показав, как посредством проникновения в национальное киберпространство можно внести хаос и сумятицу в функционирование общественных, финансовых и медиа-услуг. Когда кибератаки были уже позади, государства НАТО договорились о принятии дельнейших мер к усилению возможностей НАТО по киберзащите, включая оказание содействия технического и эксплуатационного характера государству-члену по его запросу.

Политика киберзащиты НАТО сформулирована в ряде документов высокого уровня, в которых изложены принципы, процессы принятия решений и процедуры, обеспечивающие общий согласованный подход НАТО к киберзащите и реакции на кибератаки. За принятие по необходимости и согласование незамедлительных и эффективных мер по киберзащите на уровне НАТО и между государствами отвечает Агентство по управлению НАТО по киберзащите. Одними из участников агентства являются ГЧП-структуры Североатлантического союза. Они играют важную роль в оказании помощи НАТО и партнерским странам согласно установленным процедурам, а также содействуют контактам внутри НАТО.

Особенно актуальны для НАТО кибератаки, организованные при поддержке какого-либо государства против самой организации и ее членов во время политического или военного конфликта. Реагировать на подобные кибератаки наиболее трудно, и они могут нанести немалый вред странам со слаборазвитой или маломасштабной национальной ИТ-инфраструктурой. Такие нападения способны дестабилизировать национальную безопасность, причинить значительный экономический ущерб и на многие дни или даже недели нарушить функционирование общественных и коммерческих служб. Кибератаки, совершаемые при содействии государств, также часто используются для целей шпионажа и сбора информации. В настоящее время уровень риска кибертак со стороны террористических групп считается невысоким, но ожидается, что в ближайшем будущем он возрастет.

Создание эффективных средств киберзащиты на национальном уровне технически непросто, но технически осуществимо при условии надлежащего планирования и наличии политической поддержки. Когда национальная стратегия киберзащиты уже разработана и введена в действие соответствующим законодательством, для реализации национальных средств киберзащиты потребуется формирование (1) оперативного центра, в состав которого войдут технические и оперативные службы, (2) координационного центра, где будут разрабатываться и согласовываться стратегия и концепции, происходить разрешение правовых вопросов, и поддерживаться отношения с промышленностью и международными организациями, (3) исполнительного органа, на котором будут представляться, обсуждаться и утверждаться к исполнению стратегические решения. Оперативный центр по киберзащите потребует большую часть затрат на финансирование и людских ресурсов. Затраты зависят от объема защищаемого киберпространства (например, компьютерные сети и инфраструктура) и типа услуг, предоставляемых централизованно Оперативным центром по киберзащите.

Действующий в настоящее время Центр реагирования на компьютерные инциденты НАТО обрабатывает ежедневно сотни тысяч электронных происшествий, чтобы вовремя распознать и прореагировать на действия злоумышленников. До сих пор был официально предъявлен иск по 800 инцидентам в системе кибербезопасности, ряд которых был чреват серьезными последствиями. Характер таких инцидентов – самый разный: начиная с искажений внешнего вида Интернет-сайта и заканчивая кибершпионажем и крупными взломами сети.



В ближайшем будущем НАТО планирует еще более усилить имеющиеся средства киберзащиты, усовершенствовать оказание помощи государствам и сотрудничество с промышленностью и международными организациями.

Фото: Центр киберзащиты НАТО – оперативный пункт

Участившиеся случаи пиратства в Аденском заливе и вблизи побережья Африканского Рога создают угрозу для международных гуманитарных операций, а также для безопасности морских торговых маршрутов. По запросу ООН НАТО активно содействует укреплению безопасности, предпринимая действия против пиратов в этом регионе. В своей статье Джим Капонити, председатель Совета по планированию морского судоходства НАТО, рассказывает, в чем заключается роль комитета в сдерживании пиратской деятельности. Он также повествует о других международных координационных мероприятиях.

СОДЕЙСТВИЕ В СДЕРЖИВАНИИ ПИРАТСКОЙ ДЕЯТЕЛЬНОСТИ



Задача Совета по планированию морского судоходства (СПМС) - одного из восьми советов и комитетов по планированию при Главном комитете гражданского чрезвычайного планирования (СКЕПСИ) – предоставлять консультации НАТО по антитеррористическим мерам, принимаемым для защиты объектов морского транспорта, и следить за всеми явлениями, затрагивающими безопасность коммерческого судоходства. Таким явлением в настоящее время и является пиратство, особенно близ побережья Сомали.

СПМС на уровне национальных представителей и экспертов по морскому судоходству занимается проблемой пиратства и изысканием наработок, необходимых для сдерживания пиратской деятельности. Изначально таким проблемным районом был Малаккский пролив, теперь таковыми стали

Аденский залив и воды близ побережья Сомали. Действия пиратов являются преступлениями, несущими угрозу свободе судоходства, безопасности экипажей и товаропотокам.

СПМС осуществляет обмен информацией о пиратской деятельности, анализ мероприятий по борьбе с этим явлением, консультирует по вопросам судоходства военные органы НАТО и национальные власти, собирает и распространяет информацию о передовых наработках по сдерживанию пиратства. Статус СПМС позволяет ему разрабатывать руководящие указания обязательного и рекомендательного характера для сдерживания пиратства против государств флага – членов НАТО и их партнеров.

В настоящее время принимается целый ряд мер по сдерживанию пиратской деятельности, и СПМС приветствует эти меры. Постоянное взаимодействие между правительствами стран и промышленностью должно помочь сократить число пиратских нападений и лишить пиратов возможности добиваться поставленных целей.

Борьбой с пиратством также занимается похожая структура – Контактная группа по проблеме пиратства у побережья Сомали (КГППС), учрежденная резолюцией 1851 Совета Безопасности ООН. КГППС, куда входят 28 государств и шесть международных организаций, включая НАТО, выполняет функцию координатора между государствами, региональными и международными организациями по всем аспектам борьбы с пиратством и вооруженным грабежом в море у берегов Сомали. При КГППС созданы четыре рабочие группы (РГ), которые проводят регулярные заседания и разрабатывают рекомендации по сдерживанию пиратской деятельности.

Работа руководимой Великобританией РГ-1 сосредоточена, главным образом, на военных аспектах и занимается оперативным взаимодействием и совершенствованием региональных возможностей. РГ-2, руководство которой осуществляется Данией, идентифицирует наиболее целесообразные и юридически обоснованные решения, чтобы добиваться судебного преследования лиц, подозреваемых в пиратстве. РГ-3 под руководством США занимается промышленным самоанализом и защитой. РГ-4, которой руководит Египет, работает в области общественной дипломатии и передачи информации.

В заключение следует отметить, что в борьбе с угрозой пиратства наблюдаются существенные подвижки, но остается нерешенным немало проблем. СПМС будет продолжать работать с соответствующими организациями, занимаясь борьбой с пиратством и помогая идентифицировать меры и процессы, способные помочь коммерческим перевозчикам избегать и сдерживать пиратскую деятельность и не давать пиратам добиваться поставленных целей.

Угрозы здоровью населения, такие как пандемии (вируса ВИЧ, гриппа и т.д.), не являются только национальными проблемами. В связи с этим может возникнуть серьезная угроза общественному порядку, и тогда традиционный медико-санитарный подход оказывается неэффективен. Помимо этого, государствам не решить таких проблем в одиночку, следовательно, кардинально важно международное сотрудничество. Председатель Объединенного медицинского комитета НАТО Эрик Лекарпентье рассказывает о нынешней эпидемии гриппа H1N1 и дает обзор надлежащих профилактических мер.

Грипп А(H1N1)



Грипп – контагиозное острое респираторное заболевание, вызываемое вирусами гриппа. Двадцатый век пережил три пандемии этого заболевания. Пандемия «испанки» (1918–1919 гг.) – гриппа вируса А подтипа H1N1 – охватила всю планету. Согласно данным, опубликованным на Интернет-сайте Всемирной организации здравоохранения (ВОЗ), от нее умерли около 40 млн. человек. Две последующие – «азиатский грипп» (вирус А подтипа H2N2) в 1957-1958 гг. и «гонконгский грипп» (вирус А подтипа H3N2) в 1968–69 гг. – имели гораздо менее тяжелые последствия.

Эпидемии гриппа повторяются каждую осень и зиму в странах умеренного климата. В результате ряд лиц нуждается в госпитализации, и имеются случаи с летальным исходом, в основном среди групп риска (маленькие дети, старики и лица, страдающие хроническими заболеваниями). В масштабах всего мира наблюдается от трех до пяти миллионов тяжелых и от 250 до 500 тыс. смертельных случаев. Большинство умерших от гриппа в промышленно развитых странах принадлежат к возрастной группе от 65 лет и старше. В некоторых тропических странах вирусы гриппа активны в течение всего года, причем наблюдается один - два пика активности в сезоны дождей.

Вирусы гриппа бывают трех различных типов, именуемых А, В и С. Сезонные эпидемии характерны для вирусов А и В, но вызывать пандемии может только вирус А. Вирус С вызывает спорадические случаи заболевания гриппом. Гриппозным вирусам свойственны частые мутации. Эти генетические изменения происходят при помощи двух механизмов:

- дрейф генов во время сезонных эпидемий,
- генетический сдвиг. Это явление характерно только для вирусов типа А. Именно оно обуславливает возникновение новых вирусов, от которых население не имеет защиты, что приводит к пандемиям гриппа.

Вирусы гриппа типа А подразделяются на подтипы, у каждого из которых существует особая комбинация поверхностных белков. Вирусные подтипы получают соответствующее наименование А(НхNх). Нынешняя эпидемия вызвана новым штаммом семейства А(H1N1), передающимся от человека к человеку. Он появился в результате генетической рекомбинации между вирусами свиньи, человека и птиц. Этот новый вирус отличается от вируса сезонного гриппа человека H1N1, который обычно распространяется зимой.

В северном полушарии сезонная эпидемия гриппа обычно возникает в период с ноября по апрель и продолжается в среднем 9 недель. Случаи со смертельным исходом наблюдаются, главным образом, среди пожилых людей (свыше 90% случаев приходится на возраст 65 лет или старше).

Как при пандемии, так и при эпидемии происходит резкий скачок заболеваемости за определенный период времени. Отличаются оба явления только по географическому охвату: при пандемии вирус нового подтипа, возникающий в результате генетической модификации, распространяется в масштабах нескольких континентов или всей планеты. Ввиду наличия у такого вируса новых свойств, у населения практически полностью отсутствует к нему иммунитет. Могут появляться в массовом порядке тяжелые случаи гриппа или случаи с летальным исходом. Из-за низкого иммунитета у большинства людей, им болеют чаще, чем в случае сезонного гриппа, но все же большинство заразившихся переносят грипп в легкой форме и выздоравливают без антивирусной терапии или другого медицинского лечения. Среди более тяжелых больных, свыше половины госпитализированных страдают от основных заболеваний или нарушений иммунной системы. Мы пользуемся такими понятиями, как

вирулентность – способность вируса или другого возбудителя вызывать серьезное заболевание

контагиозность – способность вируса или другого возбудителя передаваться от одного человека к другому.

Из-за всемирных масштабов эпидемии, вызванной новым вирусом гриппа А(H1N1), 11 июня 2009 г. ВОЗ объявила о переходе на этап 6 своего плана и подтвердила наличие мировой пандемии. Вирус передается от человека к человеку так же беспрепятственно, как и при обычном сезонном гриппе. Чтобы избежать распространения инфекции, больные гриппом должны закрывать нос и рот при кашле или чихании, оставаться дома, если они плохо себя чувствуют, часто мыть руки и держаться как можно дальше от здоровых людей. Науке неизвестны случаи заболевания людей в результате контакта со свиньями или другими животными. Первые симптомы инфицирования вирусом А(H1N1) – такого же типа, как и при обычном гриппе: температура выше 38°, ломота в теле, ощущение сильной усталости, кашель или проблемы

Глобальные пандемии

респираторного характера, головная боль, боль в горле и насморк, иногда понос и рвота.

При нынешней эпидемии вирус распространяется, как и при сезонном гриппе:

- воздушно-капельным путем, то есть, в результате попадания вируса в воздух при кашле, чихании или отхаркивании
- посредством прямого контакта с инфицированным (поцелуй или рукопожатие)
- путем контакта с загрязненными предметами, до которых дотрагивался больной (например, дверная ручка).

Больной гриппом является заразным с момента появления первых симптомов и далее в течение около 7 дней, инкубационный период длится также до 7 дней. В течение всего этого времени больного необходимо изолировать, и он должен надевать хирургическую маску в присутствии других людей, чтобы избежать передачи инфекции своему ближайшему окружению.

Чтобы с максимальной эффективностью локализовать распространение вируса, следует

- избегать контакта с больными
- регулярно мыть руки с мылом или дезинфицировать их с помощью спиртового раствора (который продается в аптеке или в крупных магазинах), особенно после откашливания или сморкания
- закрывать рот и нос при кашле или чихании с помощью одноразового носового платка (платок необходимо выбросить сразу после использования, желательно, в мусорное ведро с крышкой и полиэтиленовым мешком для мусора), руками или рукавом, если есть возможность их сразу же вымыть или выстирать соответственно.

Существует два типа масок:

- хирургическая, уменьшающая попадание в воздух мелких капель из верхних дыхательных путей больных. Эту маску необходимо надевать с момента появления симптомов, чтобы снизить опасность заражения окружающих – членов семьи, друзей – при кашле или чихании. Поскольку вирус распространяется воздушным путем, существует риск заражения, если человек находится напротив больного на расстоянии менее одного метра.
- маска-респиратор (стандарт FFP2) для специалистов, которые выполняют важную функцию в борьбе с пандемией и регулярно бывают в тесном контакте с больными (специалисты-медики, работники служб экстренной помощи и т. д.). Это маска одноразового использования, которая предотвращает попадание возбудителей из воздуха в верхние дыхательные пути.

В каждой стране разработаны специальные указания на случай появления симптомов. Во Франции рекомендуется обратиться к семейному врачу или позвонить в местный (на уровне департамента) неотложный медицинский координационный центр по номеру 15. В Англии создан национальный центр обработки вызовов и медицинская координационная служба. По мнению специалистов, больные подлежат изоляции и им рекомендуется оставаться дома. Госпитализироваться могут только пациенты, входящие в группы риска (беременные женщины, маленькие дети, лица с нарушениями иммунитета, пациенты в ослабленном состоянии и т. д.).

Influenza A(H1N1)

How to Protect Yourself and Others

- Cover your nose and mouth with a disposable tissue when coughing and sneezing
- Dispose of used tissues properly immediately after use
- Regularly wash hands with soap and water
- If you have flu-like symptoms, seek medical advice immediately
- If you have flu-like symptoms, keep a distance of at least 1 meter from other people
- If you have flu-like symptoms, stay home from work, school or crowded places
- Avoid hugging, kissing and shaking hands when greeting
- Avoid touching eyes, nose or mouth with unwashed hands

For more information:
<http://www.emero.who.int/csr/nr1/index.htm>
<http://www.who.int/en>

World Health Organization
Regional Office for the Eastern Mediterranean

Во время добровольной изоляции близкого родственника, заболевшего гриппом, медицинское наблюдение и регулярный мониторинг обеспечивается врачами. Членам семьи необходимо ограничить контакты с больным. Если минимальных контактов во время добровольной изоляции избежать невозможно, пациент должен надевать маску, и необходимо неукоснительно соблюдать профилактические меры (гигиенический барьер), чтобы избежать заражения, а именно

- избегать поцелуев и рукопожатий с больным
- сократить до минимума его посещения
- требовать от пациента надевать хирургическую маску, чтобы избежать попадания в воздух брызг из верхних дыхательных путей больного
- строго соблюдать гигиену рук: дома мыть руки обычным мылом (у пациента должно быть отдельное мыло) или дезинфицировать их с помощью моющего средства на спиртовой основе, особенно после каждого контакта
 - o с больным
 - o с предметами, которыми пользовался больной
 - o с личными вещами пациента
 - o с любыми поверхностями, до которых дотрагивался пациент (дверные ручки, мебель, краны и т. д.)
- хорошо проветривать жилые помещения, открывая окна
- мыть и стирать предметы обихода, которыми пользовался пациент (полотенца, столовые приборы, белье и т. д.) горячей водой с мылом или с помощью обычных моющих средств
- мыть поверхности, до которых дотрагивался пациент (дверные ручки, ручка спуска воды в туалете, пульта дистанционного управления, телефон и т. д.) горячей водой с мылом или с помощью обычных моющих средств

При плохом самочувствии, высокой температуре, кашле и/или боли в горле следует

- оставаться дома и не ходить на работу, в школу или общественные места
- пребывать в покое и пить жидкости в больших количествах
- закрывать нос и рот бумажными носовыми платками при кашле и чихании, затем их выбрасывать согласно указаниям. После этого тщательно мыть руки с мылом или с помощью спиртового раствора
- если при себе нет бумажных носовых платков для сморкания или откашливания, прикрываться рукой
- часто и тщательно мыть руки водой с мылом, особенно после откашливания или чихания
- сообщить членам семьи и друзьям о своей болезни и обратиться за помощью для выполнения повседневных дел, предполагающих контакты с другими людьми, таких как выход за покупками.

КАКИЕ СУЩЕСТВУЮТ СПОСОБЫ ЛЕЧЕНИЯ?

Только врач может принять решение о назначении той или иной терапии, в зависимости от состояния пациента. Терапия может состоять, например, только из жаропонижающего средства и гигиенических рекомендаций или противовирусного препарата. Также больному следует надевать хирургическую маску с момента появления первых симптомов, чтобы избежать заражения членов семьи и ближайшего окружения.

Поступление вакцины ожидается осенью 2009 г. Эффективными противовирусными средствами являются препараты оселтамивир (Тамифлю®) и занамивир (Реленза®). Они выдаются только по рецепту врача после медицинской консультации и постановки диагноза, с момента появления первых симптомов. Профилактическими средствами эти препараты не являются, а используются для раннего лечения гриппа. Если их принимать в самом начале заболевания, они могут ослабить гриппозные симптомы, уменьшить длительность заболевания и, возможно, предотвратить осложнения. Эти медикаменты снижают репродуктивную способность вируса, но не иммунизируют против заболевания. Основными средствами предотвращения заболевания гриппом, а также других инфекций являются вакцины. Они помогают иммунизировать реципиентов, стимулируя выработку организмом антител против вируса. Вакцина для борьбы с нынешней пандемией может появиться не ранее чем через несколько недель. Учитывая клинические испытания, выдачу разрешений на выпуск и реализацию продукции, на поставку вакцины может потребоваться около четырех месяцев с начала осени.

Совершая международные поездки, рекомендуется соблюдать осторожность при посещении стран, где подтверждено распространение вируса среди населения. Вместе с тем, Всемирная организация здравоохранения (ВОЗ) до настоящего времени не рекомендует налагать ограничения на передвижения в связи с новым гриппом А(Н1N1). В Евросоюзе какие-либо конкретные указания отсутствуют.

Населению рекомендуется:

- следовать инструкциям местных органов здравоохранения
- соблюдать элементарные правила гигиены (часто мыть руки, проветривать жилые помещения) и избегать контактов с больными людьми
- в случае повышенной температуры или гриппозных симптомов проконсультироваться у местного врача.

Программа НАТО «Наука ради мира и безопасности» объединяет ученых и экспертов из стран НАТО и их партнеров для работы на регулярной основе по программам, представляющим взаимный интерес. Программа призвана содействовать безопасности, стабильности и солидарности между странами путем применения науки к разрешению проблем. Нижеизложенный проект имеет непосредственное отношение к ГЧП в области наращивания местных потенциалов по киберзащите в партнерских странах.

НАУЧНАЯ ПРОГРАММА НАТО УКРЕПЛЯЕТ КИБЕРЗАЩИТУ В ПАРТНЕРСКИХ СТРАНАХ



Обеспечение безопасности компьютерных сетей и систем – довольно трудная задача. В ответ на любые инциденты в системе безопасности компьютерных средств организации должны действовать быстро и эффективно, чтобы минимизировать потенциальный ущерб.

Создание Групп реагирования на инциденты в системе безопасности компьютерных средств (ГРКИБ) – хороший способ расширить возможности быстрого реагирования, а также смягчить последствия будущих атак. Такие группы представляют собой небольшие структуры в составе 1-3 специалистов, имеющих соответствующую подготовку и оснащение и готовых прореагировать в самые сжатые сроки на круглосуточной основе, путем распространения важных сообщений по вопросу безопасности.

В 2006 г. по линии программы НАТО «Наука ради мира и безопасности» был инициирован проект создания таких ГРКИБ в 15 странах, у которых прежде не было систем обеспечения безопасности компьютерных средств, а именно в Азербайджане, Албании, Армении, Афганистане, Белоруссии, Болгарии, бывшей Югославской республике Македонии*, Грузии, Казахстане, Киргизстане, Молдавии, Таджикистане, Туркмении, Украине и Узбекистане.

Проект предусматривал выдачу «стартового пакета», необходимого для начала работы ГРКИБ в каждой из этих стран. В пакет входили выделенный сервер с программным обеспечением для борьбы с инцидентами, рабочая станция для персонала, маршрутизатор, коммутатор, программное обеспечение, многофункциональный принтер, бумагорезательная машина и руководства по эксплуатации. НАТО обеспечивала доставку оборудования в каждую из стран и помогала с его установкой и вводом в действие. Помимо этого, на средства НАТО можно было обучить до трех операторов групп реагирования согласно четко установленным стандартам каждой отдельно взятой страны.

Несмотря на то, что программа НМБ НАТО отвечает за общее руководство проектом и этап реализации, к работе были подключены и другие важные организации. За найм специалистов и аренду для них офисных площадей отвечали Национальные научно-исследовательские и образовательные сети (НРЕН) каждой страны. Центрально- и восточноевропейская сетевая ассоциация (ЦВЕНет), объединяющая национальные вузовские, исследовательские и образовательные сети (НРЕН) стран Центральной и Восточной Европы, Кавказа и Центральной Азии, занималась координацией закупок и поставок оборудования, а также обеспечением технического содействия в процессе его установки.

Помимо этого, все аспекты проектов тесно координировались с Европейским агентством по сетевой и информационной безопасности (ЕНИСА).

До настоящего времени результаты были весьма обнадеживающими. В большинстве стран ГРКИБ функционируют, как подобает, и за развитием ситуации осуществляется тщательный мониторинг.

Ожидается, что такого рода деятельность по линии программы НРБ НАТО продолжится в будущем с перспективой внедрения контроля средств защиты информации и их сертификации. Проект также позволит подготовить сети НРЕН и группы реагирования ГРКИБ к участию в серии мировых учений по быстрому реагированию на инциденты в системе безопасности компьютерных средств, запланированных на 2010-2011 гг. Участие в таких учениях всемирного масштаба – признание ценности работы, выполняемой группами стран-партнеров с 2006 г.

Проект служит также превосходным примером практического сотрудничества НАТО с партнерами, приносящего весомые плоды в области киберзащиты.

* Турция признает Македонию под ее конституционным названием

МЕРОПРИЯТИЯ В ГЛАВНОМ КОМИТЕТЕ ГРАЖДАНСКОГО ЧРЕЗВЫЧАЙНОГО ПЛАНИРОВАНИЯ

Осенью этого года на СКЕПСИ и подчиненных ему советах и комитетах по планированию предстоит обсудить ряд важных политических вопросов. По итогам состоявшегося в штаб-квартире организации 1-2 июля 2009 г. семинара на тему гражданской поддержки ГЧП Афганистану, СКЕПСИ вынесет на обсуждение рекомендации семинара и примет решение о путях их наиболее оптимального претворения в жизнь. В проведении данного семинара созрела необходимость, так как требовалось определить, как ГЧП-структуры НАТО, работая совместно с национальными и международными гражданскими организациями, могут помочь удовлетворить потребности в предоставлении гражданской поддержке афганским властям и ИСАФ.

За предстоящие несколько недель на основе сложившейся в целом ситуации в НАТО и результатов анализа системы ГЧП будут разработаны очередные министерские руководящие указания по ГЧП. Как было согласовано в рамках цикла планирования и анализа системы ГЧП, теперь министерские указания и рабочие программы советов и комитетов по планированию будут охватывать четырехлетний период. Рабочая программа на 2010-2013 гг. будет рассмотрена и утверждена СКЕПСИ в первом квартале 2010 г. В разработке министерских руководящих указаний, задающих ориентиры для ГЧП НАТО на ближайшие четыре года, участвуют все заинтересованные структуры. К участию в этом процессе в максимальной степени привлекаются партнеры НАТО.

Реализация проектов ГЧП продолжится в рамках практических мероприятий и семинаров. Одно из таких мероприятий – учения ЕКЦРСБК по ликвидации последствий стихийных бедствий и катастроф «ДЖЕТИСУ-2009» - пройдут с 5 по 11 сентября 2009 г. Учения проводятся с целью совершенствования оперативной совместимости среди служб экстренного реагирования и наращивания потенциала в странах НАТО и у их партнеров по борьбе со сложными чрезвычайными ситуациями. Другое важное событие – Семинар по транспорту – состоится в Бельгии 26-28 октября 2009 г., и на нем будут задействованы, главным образом, советы и комитеты по планированию, специализирующиеся в транспортной тематике (Комитет по планированию гражданской авиации, Совет по планированию морского судоходства и Совет по планированию внутреннего наземного транспорта). На этом многоплановом мероприятии планируется изучить влияние нынешней экономической ситуации на транспортную отрасль и ее использование в поддержку операций НАТО.

СКЕПСИ Текущие задачи:

- Министерские руководящие указания на период с 2010 по 2013 гг.
- Обсуждение рекомендаций семинара о предоставлении гражданской поддержке ГЧП Афганистану

ПРЕДСТОЯЩИЕ МЕРОПРИЯТИЯ

График мероприятий СКЕПСИ и Советов и комитетов планирования

- 1-3 сентября Семинар и плен.засед. К-та гражд. защиты (КГЗ) Краков, Польша
- 9-10 сентября Плен.засед. К-та по план. гражд.авиации (КПГА) Штаб-квартира НАТО, Бельгия
- 14-15 сентября Плен.засед. Совета по план.морск. судоходства (СПМС) Штаб-квартира НАТО, Бельгия
- 18 сентября Плен.засед. К-та гражд.защиты (КГЗ) Штаб-квартира НАТО, Бельгия
- 30 сент – 2 окт Мед. конф-ция НАТО Лиссабон, Португалия
- 26-27 октября Плен.засед. К-та по план. гражд.связи (КПГС)..... Штаб-квартира НАТО, Бельгия
- 26-28 октября Семинар по транспорту Антверпен, Бельгия
- 5-6 ноября Плен.засед. Объед. мед. к-та Штаб-квартира НАТО, Бельгия
- 11-12 ноября Семинар о защите энерг. инфраструктуры Вильнюс, Литва
- 12-13 ноября Плен.засед. К-та пром. планирования (КПП)..... Вильнюс, Литва
- 17-18 ноября Плен.засед. К-та прод. и с/х планирования (КПСП) Штаб-квартира НАТО, Бельгия
- 23-24 ноября Плен.засед. Совета по план. внутр.назем. трансп. (СПВНТ) Штаб-квартира НАТО, Бельгия
- 24-25 ноября Плен.засед. СКЕПСИ Штаб-квартира НАТО, Бельгия
- 3-4 декабря Заседание министров иностранных дел НАТО Штаб-квартира НАТО, Бельгия

ЕВРОАТЛАНТИЧЕСКИЙ КООРДИНАЦИОННЫЙ ЦЕНТР РЕАГИРОВАНИЯ НА СТИХИЙНЫЕ БЕДСТВИЯ И КАТАСТРОФЫ (ЕКЦРСБК)

Евроатлантический координационный центр реагирования на стихийные бедствия и катастрофы (ЕКЦРСБК) является органом партнерства, в котором страны-участницы и партнеры НАТО являются равноправными членами. ЕКЦРСБК координирует обмен информации о стихийных бедствиях и катастрофах в СЕАП. В статье обрисован новый проект, который носит название «ЭйдМатрикс». В центре этого проекта – инструмент, помогающий распространять информацию о ликвидации последствий стихийных бедствий и катастроф.

ИНСТРУМЕНТ «ЭЙДМАТРИКС»

ЕКЦРСБК достаточно давно искал техническое решение, которое позволило бы ему распространять информацию о ликвидации последствий стихийных бедствий и катастроф на современном уровне. Согласно сложившейся практике, один-два раза в сутки в центре составляются сводки и затем рассылаются среди государств СЕАП по электронной почте или по факсу. Это хорошо отлаженный способ отправки информации получателю, и данная практика, будет, естественно, продолжена. Однако, существуют и более передовые методы, с помощью которых информация размещается на виртуальной «доске объявлений» в непрерывном режиме и извлекается по запросу.

Благодаря Представительству США при НАТО, которое помогло установить контакт между ЕКЦРСБК и Фондом ЭйдМатрикс, центр смог вооружиться современным инструментом для распространения сведений о ликвидации последствий стихийных бедствий и катастроф. ЭйдМатрикс представляет собой новейший инструмент, который сокращает сроки распространения о стихийных бедствиях и катастрофах, и делает весь этот процесс более прозрачным и эффективным.

Девиз ЭйдМатрикс – обеспечивать «надлежащую помощь нуждающимся людям в надлежащие сроки». ЭйдМатрикс – некоммерческая организация, через сеть которой устанавливаются контакты между донорами и людьми, нуждающимися в помощи. Ее сеть используется 38 штатами США, Федеральным агентством США по управлению действиями в чрезвычайных ситуациях (ФЕМА), Гондурасом и Румынией. Эта сеть применяется для сбора продовольственной помощи большинством благотворительных организаций в США, а также для раздачи собранных пожертвований в форме медикаментов.

Одной из основных задач ЭйдМатрикс в области оказания помощи при стихийных бедствиях и катастрофах было создать соответствующую модель процесса и тем самым оптимизировать поток гуманитарной помощи во время реагирования



на эти ЧС и при восстановительных мероприятиях. Инструмент позволяет автоматизировать большинство трудоемких операций, выполняемых вручную. В частности, в сети ЭйдМатрикс создается единое пространство, где собирается в полном виде и размещается вся информация о потребностях, пожертвованиях и доставке в режиме реального времени, и где потенциальные доноры получают сведения о потребностях на местах и наоборот.

Процесс оказания помощи при стихийных бедствиях и катастрофах рационализируется, так как ЭйдМатрикс делает звеньями одной системы некоммерческие и правительственные организации, а также частный сектор, для координации предложений о помощи. Решение это применяется как в чрезвычайных обстоятельствах – при стихийных бедствиях и катастрофах, - так при повседневной координации благотворительных пожертвований участвующими штатами.

На таблице показано, как работает механизм главного координационного центра:

Запись внизу содержит информацию о пожертвовании 400 батареек для часов Интернет-сайтом Home Depot. Это и другие пожертвования анализируются и координируются агентством по оказанию помощи при стихийных бедствиях и катастрофах и могут быть востребованы нуждающимся в помощи зарегистрированным получателем.

Как эта система может быть применена для ЕКЦРСБК и ее функции координационного центра?

В лице нуждающихся выступает население пострадавшей страны, направившей запрос о помощи через правительственное агентство, руководящее действиями по ликвидации последствий ЧС. В лице доноров – государства СЕАП, отвечающие на запрос о помощи. ЕКЦРСБК осуществляет координацию, анализ и руководство в рамках процесса.

ЭйдМатрикс предоставил свою модель для использования в ЕКЦРСБК, после того как в июне 2008 г. СЕАП и другими партнерами был подписан соответствующий Меморандум о понимании. С сентября 2008 г. ЕКЦРСБК пользуется моделью оказания помощи при стихийных бедствиях и катастрофах в качестве дополнения ее традиционных инструментов составления сводок.

The screenshot shows the FEMA aidmatrix website interface. At the top, there is a navigation bar with links: Home, Allocation, Track Donations, Reports, Tools, Profile. A search bar is present with the text "New Donations" and "Allocation Cart". Below the search bar, there are dropdown menus for "Parent Category" and "Sub-Category", and input fields for "Donation Description" and "Company". A "Search" button and a "Show All" button are also visible.

The main content area is titled "New Donations" and contains a table with the following columns: Ref #, Donation Description, Parent Category, Sub-Category, Quantity, UOM, Company, Contact, and Date. The table lists 10 donation records, each with a "Details" link and a "Print" link.

Ref #	Donation Description	Parent Category	Sub-Category	Quantity	UOM	Company	Contact	Date
150	1 month of cooking	Services	Food Services -Skilled-- Cooking	2.00	Each	Aidmatrix	TXprivatedonor	04/27/2007
158	vegetables & fruits	Food	Canned Goods	3.00	Cases	Test 123	TXprivatedonor	04/27/2007
166	Unskilled Tools	Services	With Tools -Unskilled-- with Other Tools	12.00	Cases	Accenture	Rob Saunders	04/27/2007
168	Asbestos to make a bad situation worse	Services	Hazardous Materials - Skilled-- Asbestos	12.00	Each	Accenture	Rob Saunders	04/27/2007
170	AAA batteries	Electrical	Batteries	4.00	Each	ACN	Steph	04/27/2007
171	10 boxes of size 4 diapers	Apparel	Baby Diapers	10.00	Each	Accenture	TXprivatedonor	04/27/2007
182	My house	Shelter	Private Home	1.00	Each	ACN	This Guy	04/27/2007
183	10 boxes of diapers	Apparel	Baby Diapers	10.00	Each	accenture	Kristin	04/27/2007
184	Technical Services for Software Installation	Services	Information Services - Skilled-- Software- Computer	1.00	Each	Big Iron Computers	TXprivatedonor	04/27/2007
185	Used watch batteries	Electrical	Batteries	400.00	Each	Home Depot	John Donor	04/27/2007

At the bottom of the table, there are page navigation numbers: 1 2 3. The browser status bar at the bottom indicates "Internet | Protected Mode: Off" and "100%".

ГЧП в других международных организациях

Так как НАТО не единственная организация, действующая в области гражданского чрезвычайного планирования, в данной таблице размещены полезные ссылки на другие организации, которые также трудятся в данной сфере.

ОРГАНИЗАЦИЯ	ИНТЕРНЕТ-САЙТ
Европейская Комиссия	http://ec.europa.eu/environment/civil
	http://ec.europa.eu/dgs/justice_home/terrorism/dg_terrorism_en.htm
Центр мониторинга и информации Евросоюза (ЦМИ)	http://ec.europa.eu/environment/civil/prote/mic.htm
Управление по гуманитарной помощи Еврокомиссии	http://ec.europa.eu/echo/index_en.htm
Управление ООН по координации гуманитарных вопросов (УКГВ ООН)	http://ochaonline.un.org
Организация по безопасности и сотрудничеству в Европе (ОБСЕ)	http://osce.org
Международное агентство атомной энергии (МАГАТЭ)	http://iaea.org
Центр по инцидентам и аварийным ситуациям МАГАТЭ (ЦИАС)	http://www-ns.iaea.org/tech-areas/emergency/incident-emergency-centre.htm
Руководящие указания МАГАТЭ для служб экстренного реагирования в случае радиационных аварийных ситуаций	http://www-ns.iaea.org/tech-areas/emergency/emergency-response-actions.asp
Организация по запрещению химического оружия (ОЗХО)	http://www.opcw.org

КУРСЫ И ДРУГИЕ МЕРОПРИЯТИЯ ПО ГЧП

Ниже размещен перечень предстоящих мероприятий в других международных организациях:

ОРГАНИЗАЦИЯ	МЕРОПРИЯТИЕ	ДАТЫ	МЕСТО
ОЗХО	Курс по оказанию помощи и защите	7-11 сентября	Куопио, Финляндия
Спасательная служба Швеции	Курс по международным экологическим катастрофам	7 сентября	подлежит уточнению, Швеция
Федеральное управление по гражданской защите и оказанию помощи при стихийных бедствиях, Германия	5й Европейский конгресс по гражданской защите и управлению действиями при стихийных бедствиях и катастрофах	5-6 ноября	Бонн, Германия
Школа НАТО	Курс НАТО по гражданскому чрезвычайному планированию	16-21 ноября	Обераммергау, Германия
Школа НАТО	Курс НАТО по защите от терроризма	23 ноября	Обераммергау, Германия
Европейская Комиссия	3й Форум по гражданской защите	25-26 ноября	Брюссель
МАГАТЭ	Укрепление глобального режима ядерной и физической безопасности	14-18 декабря	Кейптаун, ЮАР
Уилтон Парк	Рациональная энергетическая политика Евросоюза	3-12 декабря	Уилтон Парк, Великобритания

С дополнительной информацией можно ознакомиться через e-Prime - Партнерскую систему управления и обмена информацией в режиме реального времени.