Иван ЮРКИН:

«Кибертерроризм — вызов XXI века»

Опасность международного терроризма состоит в том, что он не знает государственных границ, поэтому бороться с ним можно только сообща, задействовав ресурсы всего мирового сообщества. Для этого необходима координация усилий правительств и спецслужб многих государств. Надо учитывать, что террористы постоянно совершенствуют арсенал средств и методов своей деятельности. Сегодня все большую угрозу представляет кибертерроризм, становясь вызовом XXI века.

Наш сегодняшний собеседник – генерал-майор КГБ запаса Иван Юркин *(на снимке)*, который возглавляет антитеррористический отдел Департамента СНГ по сотрудничеству в сфере безопасности и противодействия новым вызовам и угрозам. В сфере борьбы с терроризмом Иван Захарович прошел серьезную практическую школу. Многим памятны события 11 июня 1996 года, когда 43-летний террорист Александр Зюльков, угрожая взрывным устройством, захватил в заложники пятнадцать детей и двух воспитательниц детского сада № 511 города Минска. Одну из ключевых ролей в освобождении заложников и ликвидации террориста сыграл в то время начальник криминальной милиции — заместитель министра внутренних дел, а впоследствии первый заместитель Государственного секретаря Совета Безопасности Беларуси генерал-майор Иван Юркин. Именно он возглавил штаб по освобождению заложников, лично вел переговоры с террористом, который в результате профессиональных действий представителей спецслужб был ликвидирован, а заложники освобождены...

— Иван Захарович, события 11 сентября 2001 года показали, что международным террористическим угрозам можно противостоять только сообща, задействовав ресурсы всего мирового сообщества. С какими новыми вызовами приходится сталкиваться сегодня в борьбе с международным терроризмом?

— Не сбрасывая со счетов другие угрозы, я бы выделил кибертерроризм, использование Интернета в преступных целях. Этот сектор преступной деятельности стремительно набирает обороты в современном обществе, а совокупный ущерб от него уже исчисляется десятками миллиардов долларов. В США финансовые убытки от «фишинга» в прошлом году превысили 2,8 миллиарда долларов.

В 1998 году террористические организации поддерживали в Интернете лишь 12 сайтов. Сейчас их количество увеличилось примерно до 4800.

Различные террористические структуры научились эффективно работать в электронном пространстве: они часто создают сайты-однодневки, меняют форматы и адреса. К примеру, многочисленные попытки спецслужб США выдавить «Аль-Кайду» из всемирной сети заканчивались неудачами. На своих сайтах террористы не сообщают о своих действиях и их результатах, вместо этого они ведут информационно-психологическую войну против своих противников.

Сайты террористических группировок активно используются для рекрутирования новых членов и сбора пожертвований. Интернет также используется ими для разведывательных целей: по оценкам американских ученых, в Интернете содержится до 80 % информации, необходимой для организации успешной террористической атаки. В сети размещаются различные инструкции, например, по самостоятельному изготовлению взрывных устройств террористического характера, присутствующих в Интернете, являются русскоязычными.

— Бок о бок с кибертерроризмом идет ядерный терроризм...

— Именно. Это еще один вид терроризма, который можно отнести к особо опасным угрозам. Данный факт необходимо учитывать при намечающемся строительстве АЭС в Беларуси. В свое время глава Антитеррористического центра государств – участников СНГ Борис Мыльников отмечал, что возможность использования кибертерроризма в ядерном преломлении в наше время не так уж фантастична, последствия могут иметь катастрофический характер, о чем свидетельствуют факты чрезвычайных происшествий, связанных с применением компьютерных технологий в атомной энергетике и промышленности. Напомню о внедрении злоумышленниками в компьютер Игналинской АЭС в Литве электронного вируса, в результате чего могла произойти авария, подобная чернобыльской. В этом смысле белорусы, больше всех пострадавшие от аварии на ЧАЭС, наиболее остро осознают, что в ядерных технологиях не должно быть уязвимых для террористов мест.

— Беларусь готова к противодействию подобным угрозам?

— Еще в январе 2002 года, выступая на итоговой коллегии, министр внутренних дел генерал-лейтенант Владимир Наумов отметил, что вызывает беспокойство перенос на территорию нашей страны деятельности транснациональных организованных преступных групп, занимающихся распространением оружия массового поражения и его компонентов. В 2001 году в системе криминальной милиции Беларуси было сформировано подразделение по противодействию компьютерной преступности. Уже в тот период подразделением была установлена преступная группа из 26 человек и 5 ее организаторов, которые совершали хищения в Интернет-магазинах США, Новой Зеландии, ФРГ, Австралии компьютерной техники, цифровых фотокамер. Всего тогда было совершено более 70 хищений...

И все же особый акцент я бы сделал на координации международных усилий в борьбе с терроризмом в целом и унификации законодательства в данной сфере, в первую очередь в рамках СНГ, ведь тот же кибертерроризм является другой произвольной время террористического инте национала, противостоять ко рому мы можем только общи усилиями. К числу документ служащих основой для осущес ления взаимодействия компет тных органов государств Сод жества в вопросах предупреж ния, выявления, пресечения расследования актов террор ма, относится Договор о сотр ничестве государств – участ ков СНГ в борьбе с терроризм подписанный 4 июня 1999 го Он ратифицирован 8 государст ми Содружества из 9 подпис ших.

— Иван Захарович, давай резюмируем: какие первоо редные задачи необходимо шить для успешного проти действия кибертерроризму

— Еще в прошлом году в Мос по инициативе МВД России стоялась международная пра ческая конференция по борьб киберпреступностью и киберт роризмом. Международная вст ча проводилась в рамках пред дательства Российской Феде ции в «группе восьми», в ней п няли участие представит 32 государств мира, в том чи Исполнительный комитет СНГ, торый довелось представлять И тогда, и сейчас на повестке стоят вопросы сближения под дов различных государств к вы ботке совместных практичес мер по борьбе с киберпреступ стью и кибертерроризмом. Р идет о защите критических и раструктур, противодействии законному использованию Интернет в целях пропаганды совой и религиозной розни, бовки террористов и их фина рования, а также торговли л ми, оружием и наркотиками. менее актуальным является сечение мошенничества в сф электронных платежей, борь распространением вирусных грамм и хищениями персон ных данных, противодействие пространению детской порно фии, борьба с нарушениями торских и смежных прав в сф информационных технологий

Наша первоочередная зада проводить накопление и ан материалов по киберпреступ ти и кибертерроризму, разви нормативно-правовую базу трудничества государств – уч ников СНГ. Могу отметить, государства – участники Со жества занимают в этой сф активную позицию и готовы к тиводействию любым возни щим угрозам.

Юркин, И. «Кибертерроризм – вызов XXI века» : [беседа с генерал-майором КГБ Иваном Юркиным] / Иван Юркин ; беседовал Николай Левчук // Рэспубліка. — 2007.— 5 красавіка. — С.3.