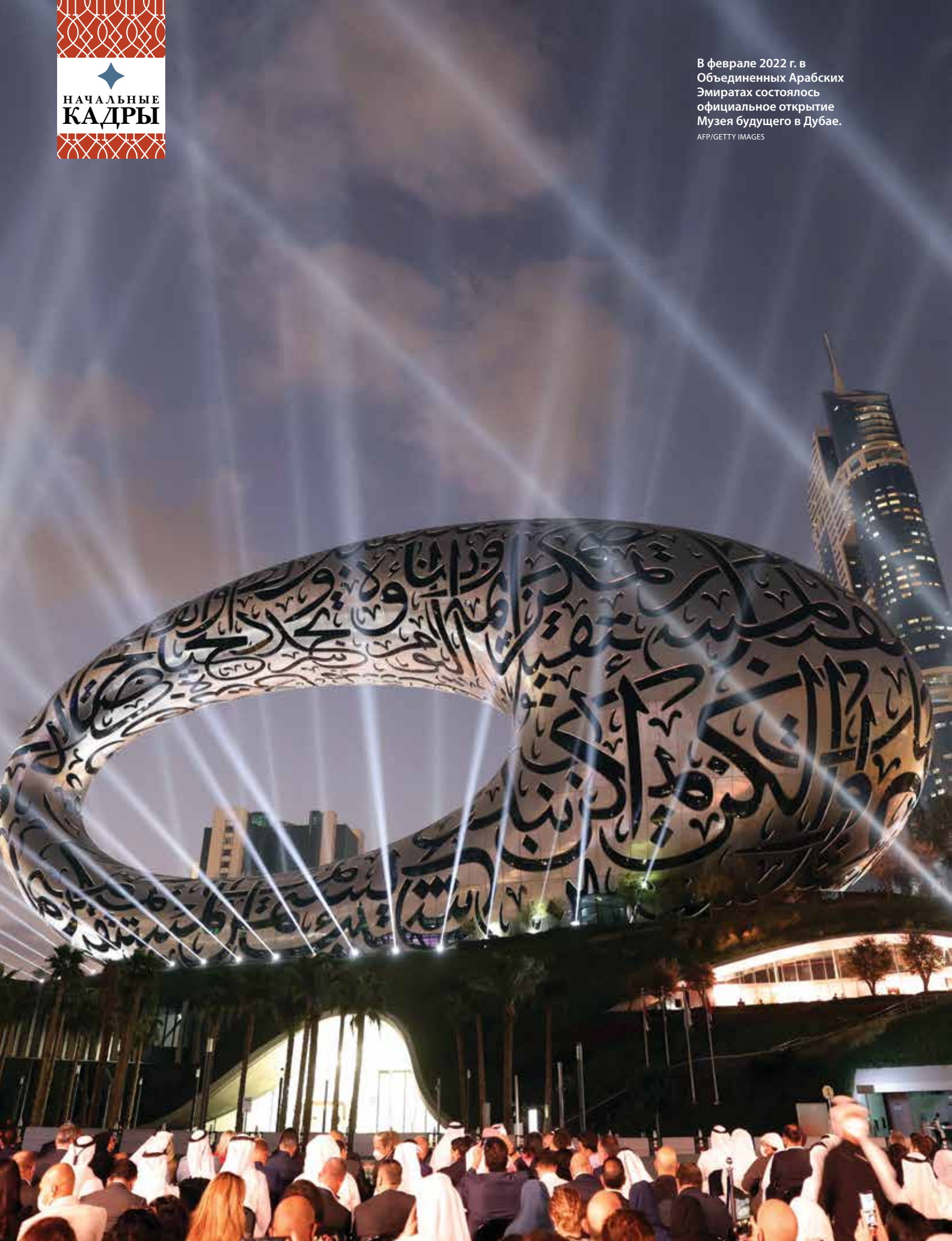
Катар проводит операцию по спасению беженцев

Военно-морские силы Иордании защищают водные пути

На защите территориальной целостности Йемена

UNIPATH

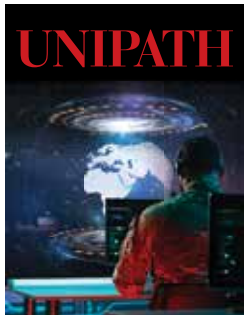
ОБЕСПЕЧИВАЯ БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА



В феврале 2022 г. в Объединенных Арабских Эмиратах состоялось официальное открытие Музея будущего в Дубае.
AFP/GETTY IMAGES

Казахская женщина празднует Новруз, древний праздник, знаменующий весеннее равноденствие. Алматы, март 2022 г. РЕЙТЕР

СОДЕРЖАНИЕ



НА ОБЛОЖКЕ:
В число защитных функций военных также входит защита общества от кибернападений и вербовки террористов через интернет.
ИЛЛЮСТРАЦИЯ «UNIPATH»

UNIPATH

Обеспечивая безопасность киберпространства

Том 11, Номер 4

КОМАНДУЮЩИЙ ОБЪЕДИНЕННОГО ЦЕНТРАЛЬНОГО КОМАНДОВАНИЯ

Генерал Майкл «Эрик» Курилла
Сухопутные силы США

СВЯЖИТЕСЬ НАМИ:

Unipath
c/o Commander
U.S. Central Command
7115 S. Boundary Blvd.
MacDill AFB, FL 33621
USA

CENTCOM.UNIPATH@MAIL.MIL

«**Unipath**» - это ежеквартальный профессиональный военный журнал, публикуемый Командующим Центрального командования США. Он является международным форумом для военнослужащих в регионе Ближнего Востока и Центральной и Южной Азии. Мнения, высказываемые в этом журнале, не обязательно отражают политику или точку зрения Командования либо любого другого ведомства правительства Соединенных Штатов. Предложенные статьи написаны персоналом «Unipath»; при необходимости, указываются другие источники. Министр обороны постановил, что публикация данного журнала необходима для связи Министерства обороны с общественностью, в соответствии с законодательством США.

ISSN 2333-1976 (печать)
ISSN 2333-1984 (онлайн)

СООБЩЕНИЕ КЛЮЧЕВОГО ЛИДЕРА

Я хотел бы выразить признательность Центральному командованию США за предоставленную мне возможность написать вступительную статью для этого выпуска журнала «Unipath», посвященного вопросам защиты киберпространства. Чем быстрее наш мир движется вперед и чем больше он зависит от технологий, тем больше возрастает риск наступления хаоса, если будут выведены из строя компьютеры и серверы, управляющие онлайновой инфраструктурой. Это касается транспортных услуг, электроснабжения, газоснабжения, опреснительных сооружений и сетей финансовых услуг, оказываемых банками, биржами и финансовыми центрами. Нарушить их работу могут враждебные субъекты или природные катастрофы, и приведет это к кошмару, который может отбросить мир назад в каменный век.

Сбои в работе серверов, принадлежащих некоторым технологическим гигантам, вебсайтов социальных сетей и приложений демонстрируют всю хрупкость современного мира, в котором люди чувствуют себя одинокими, изолированными и опустошенными. Это также показывает степень нашей зависимости от социальных сетевых ресурсов и подвергает опасности само наше существование, загоняя нас в ситуацию «быть или не быть». И к таким угрозам мы должны быть готовы.

Возможно, пандемия коронавируса и ее смертоносные последствия вызвали страх у человечества от того, что всем настоятельно рекомендовали соблюдать социальную дистанцию, переходить на удаленный режим работы и все больше использовать приложения для видео, аудио и других видов коммуникаций. Все это повысило озабоченность относительно защиты киберпространства – в этой конфронтации с самой природой кибербезопасность превратилась в жизненно важную битву за обеспечение благосостояния человечества.

Мир должен быть готов к таким сценариям и рассматривать их в качестве глобальной войны, которую мы должны вести. Роль армий больше не ограничивается противостоянием потенциальным угрозам, она также включает в себя изучение направлений и траекторий движения для того, чтобы разработать соответствующие планы реагирования на возникающие угрозы, и самым основным из них должен быть план обеспечения кибербезопасности ради сохранения человеческой цивилизации. Сегодня это уже жизненно важный вопрос, и мы обязаны защитить киберпространство всеми доступными средствами.

Кибервойна включает в себя шпионскую деятельность в отношении государств, похищение торговых и военных секретов, нападение на компьютеры, отвечающие за работу критически важной инфраструктуры и систем вооружения, похищение важной информации, связанной с вопросами безопасности и экономики, а также нападение на ключевые службы и объекты национальной безопасности стран-противников.

Эта война нового типа проходит на полях сражения на суше, в воздухе и на море. Для противостояния этим нападениям необходимы слаженные усилия всех государственных учреждений как единой мощной, труднопробиваемой системы обороны.

В былые времена человеческие знания приумножались за десятилетия или даже века. Сейчас же, благодаря информационной революции, приумножение знаний происходит ежечасно, и этот непрерывный и быстрый прогресс, достигнутый человечеством, каждый день несет в себе не только новые возможности, но и новые угрозы.

Побочным продуктом цифрового века является тенденция к использованию некоторыми правительствами, организациями и индивидуумами современных технологий во зло, ради разрушения, что является вопиющим нарушением прав человека и международных договоров и уставов. Такие действия во многом стали возможными из-за отсутствия международного консенсуса. Поэтому необходимо, чтобы институты мирового сообщества взяли на себя ответственность по защите технологических достижений от злодеев, как государств, так и отдельных лиц, и начали работу над созданием органа по наблюдению за нарушающими законы государствами, организациями и индивидуумами и над привлечением их к ответственности в соответствии с международным законодательством.

Мы в государстве Кувейт очень серьезно относимся к вопросу защиты киберпространства. На своем заседании 31 мая 2021 г. совет министров страны одобрил создание Национального центра кибербезопасности и дал распоряжение министру иностранных дел и государственному министру по работе правительства, при содействии других соответствующих министерств и госучреждений подготовить проект указа об официальном объявлении о создании указанного центра.

Этот центр отвечает за объединение и координацию усилий всех государственных ведомств по защите киберпространства от нападений, которые можно ожидать в нынешних условиях глобального киберхаоса.

Все национальные институты также должны иметь тактические задачи обеспечения безопасности собственных сетей и стратегические задачи участия в защите киберпространства государства и работы в рамках единого органа под эгидой Национального центра кибербезопасности.

На уровне Министерства обороны партнерские отношения между армией Кувейта и Центральным командованием США в сфере технологий информационной безопасности являются примером должного международного сотрудничества. Мы регулярно проводим учебные курсы, семинары и совместные мероприятия, направленные на снижение рисков и защиту информационных систем и внутренних сетей.

Кибербезопасность не является задачей какой-то одной страны, ею должна заниматься коалиция международных партнеров, имеющих технологии и «ноу-хау» для противодействия постоянно эволюционирующим угрозам компьютерным системам, от которых так зависимы мир и человеческая цивилизация.

Генерал-лейтенант Мухаммед Акла Аль-Анези,
Командующий армейским корпусом связи Кувейта

КОЛЛЕКТИВНАЯ ОБОРОНА: точка зрения Киберкомандования США

ГЕНЕРАЛ-ПОЛКОВНИК ЧАРЛЬЗ МУР, ЗАМЕСТИТЕЛЬ КОМАНДУЮЩЕГО КИБЕРКОМАНДОВАНИЕМ США

В ноябре 2020 г. более 158 млн. граждан США участвовали в наших национальных выборах. Поскольку выборы являются одной из основ нашей демократической республики, американцы должны быть уверены в том, что процесс выборов и их результаты не подвержены иностранному вмешательству и что тайные попытки иностранных сил повлиять на выборщиков нейтрализованы. Четырьмя годами ранее враждебные субъекты пытались посредством операций в киберпространстве повлиять на голоса избирателей.

ГЕНЕРАЛ-ПОЛКОВНИК ЧАРЛЬЗ МУР

Исполненные решимости предотвратить подобные действия во время национальных выборов 2018 г. и 2020 г., правительственные учреждения США создали единую многофункциональную группу для выявления угроз, обмена информацией и координации действий. В создании этой группы принимали участие такие ведомства как Агентство по кибербезопасности и безопасности инфраструктуры, Федеральное бюро расследований, Агентство по национальной безопасности и Киберкомандование США (КИБЕРКОМ).

Кроме того, для повышения эффективности усилий эта группа работала в тесном сотрудничестве со странами-союзниками и партнерами среди промышленных компаний. Это сотрудничество представляет собой пример коллективной обороны, которая необходима для защиты наших демократических процессов и страны в целом.

Для защиты нашей страны в киберпространстве КИБЕРКОМ применяет стратегический и оперативный подход под названием «передовая оборона». Из-за глобальной природы, присущей киберпространству, большинство угроз нашему государству создается в киберпространстве других стран, также известном как «красное пространство». Противостояние угрозам XXI века требует оперативности и динамичности, а также отношений партнерства для поиска и обнаружения противника в «красном пространстве» до того, как он нанесет удар по информационным системам, оружейным системам и сетям Соединенных Штатов и их союзников. Проще говоря, мы предпочитаем выставить своих лучников, чем уворачиваться от стрел противника. Собранные нами в ходе операций разведданные передаются другим правительственным ведомствам, а также нашим партнерам и союзникам с тем, чтобы у всех нас были единое понимание ситуации относительно потенциальных угроз, хорошо скоординированные усилия и возможность принятия совместных слаженных ответных мер.

Так же как единство необходимо при ведении других боевых действий, оно крайне необходимо и для успешных операций в киберпространстве, и в этом отношении очень важны партнерские отношения. Поэтому не удивительно, что развитие партнерства является ключевым компонентом стратегического подхода Национальной стратегии обороны США и КИБЕРКОМ. Поскольку киберпространство пронизывает сегодня все сферы общества, то его защиту мы называем «самым важным командным видом спорта». Крайне необходимо развивать и совершенствовать наши партнерские отношения между правительственными ведомствами США и странами-союзниками, представителями

промышленности и учеными с тем, чтобы объединить усилия в единый прочный комплекс.

Одним из способов, которыми КИБЕРКОМ создает партнерские отношения в рамках коллективной безопасности, является использование т.н. «операций передовой охоты». По приглашению страны-партнера мы направляем туда команду опытных кибервоинов для ведения «охоты» за злоумышленниками в сетях партнера. В рамках этого мероприятия наша киберкоманда собирает важную разведывательную информацию и выявляет потенциальные угрозы для наших собственных сетей, одновременно с этим помогая принимающей стране усовершенствовать защиту и жизнестойкость своих сетей.

В заключении каждой «операции передовой охоты» наша команда представляет принимающей стране отчет о ее уязвимых сторонах и рекомендуемой стратегии по предотвращению хакерских атак на ее сети. Собранная командой информация о тактике, методах и процедурах противника, а также о попытках нарушить работу систем при помощи вредоносных программ распространяется также и среди агентств по кибербезопасности по всему миру. Иногда в результате «операций передовой охоты» удаётся вычленить образцы вредоносных программ, которые КИБЕРКОМ может публиковать для того, чтобы национальные сети и сети стран-партнёров научились защищаться от возможных попыток их взломать.

Мы начали проводить «операции передовой охоты» в 2018 г. в рамках наших усилий по защите выборов, и теперь проводим их во многих странах.

Еще одним способом усовершенствования наших партнерских отношений в коллективной обороне являются учения, на которых отрабатываются вопросы взаимодействия и готовности к отражению кибератак. Как при проведении любой военной операции, важно, чтобы союзники и страны-партнеры постоянно проходили совместное обучение, чтобы ознакомиться с сильными и слабыми сторонами, а также с тактикой, методами и процедурами друг друга. Цель состоит в том, чтобы наше взаимодействие проходило беспрепятственно.

В ноябре 2021 г. КИБЕРКОМ организовало у себя самые крупные на сегодняшний день совместные многонациональные киберучения «Киберфлаг 21-1». На учениях этой серии проверяются и совершенствуются навыки и способность защищать компьютерные сети более 200 кибервоинов из 23 стран, предлагая им отреагировать на сложные сценарии в киберпространстве. На таких учениях мы оттачиваем у участников коалиции такие качества как оперативность, точность, мобильность и единство действий, которые необходимы для коллективной защиты наших стран.

Эффективная оборона киберпространства также требует тесных партнерских отношений с частным сектором. КИБЕРКОМ сотрудничает с частными компаниями через две основные программы – «Under Advisement» и «Dreamport». «Under Advisement» – это открытая, добровольная и взаимовыгодная программа обмена информацией с частным сектором. «Dreamport» – это несекретный

Гражданка США на избирательном участке. Нью-Йорк, 2020 г. Надежная защита выборов от иностранного влияния является одной из задач Киберкомандования США. GETTY IMAGES

инновационный центр, позволяющий КИБЕРКОМ взаимодействовать с представителями промышленных и научных кругов и обмениваться мнениями и новаторскими методами решения проблем кибербезопасности. Обе программы вносят непосредственный вклад в повышение способности КИБЕРКОМ защищать нашу страну в киберпространстве и в его дальнейшее развитие по всем направлениям деятельности.

Программа «Dreamport» представляет собой один из способов, которыми КИБЕРКОМ извлекает пользу из партнерских отношений с академическим сообществом. Командование недавно создало официальную Сеть сотрудничества с академическими кругами, в которую вошла 91 научная организация. Эта сеть предусматривает сотрудничество в сфере новаторских решений технических проблем и новой аналитической информации о враждебных киберсубъектах, что будет способствовать нашим коллективным усилиям по защите систем. Эта сеть также окажет положительный воздействие на найм рабочей силы, поскольку будет давать студентам возможность ознакомиться с перспективой сделать успешную карьеру в военном или гражданском секторе кибербезопасности.

Безусловно, защита сетей Министерства обороны США и страны в целом от вредоносных киберсубъектов требует коллективного подхода. Этот коллективный подход, в свою очередь, требует тесного сотрудничества между правительственными ведомствами, нашими союзниками, промышленностью и научными кругами.

Наша способность беспрепятственно и быстро обмениваться информацией, постоянно проводить совместные учения и операции и развивать новаторские подходы ко всем нашим проблемам в сфере кибербезопасности чрезвычайно важна для того, чтобы мы могли успешно выполнять нашу миссию по обеспечению кибербезопасности и защите страны в XXI веке. ✦

НАСИЛИЕ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Террористы, преступники и враждебные государства используют киберпространство в качестве поля боя для дестабилизации общества

ИЛЛЮСТРАЦИЯ «UNIPATH»

ИСЛАМСКАЯ КОАЛИЦИЯ ПО БОРЬБЕ С ТЕРРОРИЗМОМ

В глобальном масштабе Интернет децентрализован, что создает условия анонимности и позволяет использовать его в качестве платформы для незаконной деятельности, включая преступления против собственности и пропаганду насильственного экстремизма. Перед лицом такой уязвимости – возможности использования Интернета в своих интересах экстремистами и террористами – правительства столкнулись с необходимостью сдерживания этих преступников, стремящихся подорвать легитимность государства и совершать акты насилия.

Для многих правительств кибертерроризм является угрозой номер один; из-за глобальной зависимости от информационных технологий он наносит огромный ущерб. Основными мишенями кибертерроризма могут быть правительства и правительственные учреждения, банки, инфраструктура коммуникаций, а также коммунальные услуги, такие как водоснабжение, электроснабжение и нефтегазовые объекты. Нападение на них может привести к огромному экономическому, политическому и физическому ущербу.

Группировки кибертеррористов стали более хитрыми и скоординированными. Для поддержания любого своего нападения они могут использовать любые подключенные к Интернету компьютеры. Таким образом, кибертерроризм стал угрозой для крупных организаций и всех граждан, пользующихся компьютерами.

Кибероперации привлекают террористов по нескольким причинам. Они менее дорогостоящие по сравнению с традиционными террористическими

методами, поскольку почти все, что для них требуется – это подключенный к Интернету персональный компьютер. Нет необходимости покупать оружие или взрывчатку. Одним из наиболее распространенных методов электронного терроризма является создание и передача компьютерных вирусов по обычным телефонным линиям или через беспроводные коммуникации, что может нарушить работу важных систем с такой же результативностью, как и взрыв бомбы.

Определение кибероружия по-прежнему остается двусмысленным. Оно находится в мутной зоне программных кодов, используемых в преступных целях. Проводя различие между оружием и инструментом, необходимо принимать во внимание намерение преступника, которое состоит в причинении вреда посредством разрушения или устрашения. Это является неотъемлемой частью определения кибероружия.

Например, молоток представляет собой инструмент, используемый для целого ряда целей. Если молоток используется для нанесения телесных или материальных повреждений, то он становится опасным оружием. Эта логика может применяться также и к программному обеспечению, которое совершенно безвредно в одних случаях и становится разрушительным оружием в других, когда используется в враждебных целях.

Размер нанесенного кибероружием ущерба измеряется зависимостью населения от сети, ставшей объектом нападения. Поэтому, ущерб, нанесенный кибероружием критически важной инфраструктуре, например, электрическим сетям, будет очень серьезным.

Всегда существует риск, что это оружие попадет в руки террористических организаций. Например, группа, известная под названием «Shadow Broker», взломала сеть Агентства США по национальной безопасности и утверждала, что похитила национальное кибероружие с целью продать его потом на аукционе. Поэтому можно предположить, что через виртуальных «торговцев оружием» кибероружием можно торговать как обычными вооружениями.

Общим всеохватывающим термином для любого типа программного обеспечения, созданного с целью нанесения вреда или использования в неблаговидных целях программируемого устройства, сервиса или сети, является вредоносное программное обеспечение. Обычно оно используется киберпреступниками для добывания информации с целью получения финансовой выгоды. Стремятся получить данные, относящиеся к области финансов или здоровья, электронную переписку и персональные пароли. Преступников может интересовать абсолютно любая информация.

ВИДЫ НАПАДЕНИЯ

Одним из наиболее коварных способов захода в систему для нанесения ущерба является использование атаки нулевого дня – обнаружение уязвимости программного обеспечения, защита от которой еще не была создана. Помимо создания и применения вредоносных и шпионских программ, эта уязвимость может использоваться хакерами для получения доступа к секретной информации. Распределенные атаки «Отказ в обслуживании», похищение данных и другие виды вторжения в систему могут осуществляться ботнетами. Ботнеты, или боты – это несколько подсоединенных к Интернету устройств, причем каждое из устройств управляет одним или несколькими ботами. Тот, кто осуществляет нападение, может управлять роботами при помощи программного обеспечения контроля и управления.

Самым известным и самым старым видом вредоносных программ являются вирусы. Это внедренные в компьютеры или файлы программы, которые размножаются и заражают другие файлы или компьютеры и могут уничтожать и удалять данные. Компьютер может оставаться неинфицированным до тех пор, пока не будет запущена вредоносная программа, а вирус может находиться в неактивном состоянии до тех пор, пока инфицированные файл или приложение не будут открыты. Для распространения вируса и заражения других файлов или систем от пользователя требуются определенные действия, такие как, например, рассылка инфицированной программы с использованием списка рассылки.

Террористы часто нападают на своих жертв, используя кибердиверсии, называемые «логическими бомбами», когда в систему внедряется программное обеспечение, которое при создании определенных условий начинает свою разрушительную деятельность. «Логические бомбы» могут применяться не только с целью причинения вреда, но, например, также и для того, чтобы после окончания оговоренного периода апробации бесплатная пробная программа выводилась из строя. Террористы понимают важность «логических бомб»; функционирование инфраструктуры в большей части мира зависит от компьютерных сетей, и специальные атаки с использованием «логических бомб» могут нарушить работу многих глобальных банковских и транспортных систем.

ПОД ПРИЦЕЛОМ ИНФРАСТРУКТУРА

Критически важная инфраструктура обеспечивает оказание необходимых обществу базовых услуг, таких как транспорт, производство продуктов питания и электроэнергии, а также услуги здравоохранения. Серьезное повреждение сетей таких услуг может поставить большое количество людей в уязвимое положение. Зависимость этих услуг от электронных цепочек поставок еще больше усугубляет отрицательные последствия кибернападений, поскольку эти услуги являются основой национальной экономики, особенно такие сферы как безопасность, здравоохранение, энергоснабжение, водоснабжение, транспорт, грузоперевозки, коммуникации, а также банковские и финансовые услуги.

Критическая инфраструктура может оказаться уязвимой к нападениям кибертеррористов. Возрастающая доступность и взаимозависимость информации в

Распознавая экстремистские платформы в социальных сетевых ресурсах

ИСЛАМСКАЯ КОАЛИЦИЯ ПО БОРЬБЕ С ТЕРРОРИЗМОМ

Онлайновые социальные сети стали доминирующей платформой для коммуникаций: «Фейсбук» насчитывает миллиарды пользователей, «YouTube» 2,2 млрд. пользователей, WhatsApp 2 млрд., «Messenger» 1,3 млрд., и «Instagram» 1,2 млрд. пользователей. Ежемесячно почти 4 млрд. человек используют эти платформы для коммуникаций. Использование социальных сетей растет как снежный ком, делая их излюбленным методом насильственных экстремистов при вербовке новых членов. Правительства, стремящиеся бороться с терроризмом, игнорируют социальные сети, что является серьезной ошибкой. Для противостояния попыткам идеологических экстремистов вербовать сторонников через Интернет они должны брать на вооружение нарождающиеся технологии, такие как искусственный интеллект (ИИ).

ТЕРРОРИЗМ И СОЦИАЛЬНЫЕ СЕТИ

Бывший министр внутренних дел Великобритании Эмбер Радд характеризует борьбу с экстремистским контентом в режиме онлайн как своеобразную гонку вооружений между экстремистами и правоохранительными органами. По данным Радд, к ноябрю 2017 г. насильственные экстремисты запустили примерно 40 тыс. вебсайтов и приложений. Как и в любой гонке вооружений, здесь требуются самые современные технологии.

Представляем вам новую технологию под названием «Диолог ИИ», которая представляет собой исследовательский проект, нацеленный на обнаружение и удаление экстремистского онлайн-контента в максимальной степени. Следует отметить, что обучение аппаратуры достижению этих целей позволило значительно сократить объем такого контента.

Технологические гиганты во главе с «Майкрософт», «Google», «Фейсбук», «Амазон» и «Твиттер» объявили о своей поддержке международной инициативы, известной как «Christchurch Call», которая выступает против экстремистского контента в Интернете. Эти компании демонстрируют свою безоговорочную приверженность постоянному обновлению своих правил пользования и внедрению разнообразных способов уведомления об обнаруженном контенте экстремистского характера и инвестированию в технологии мониторинга.

Координационный комитет Контртеррористичесого управления ООН запустил инициативу «Антитеррористические технологии», которая активно отслеживает более 500 экстремистских каналов на более чем 20 контентных платформах и месседж-приложениях.

Террористические группировки используют платформы социальных сетей для самых разнообразных целей. Они занимаются сбором средств, укрепляют свою коллективную идентичность и объединяют усилия своих членов. Эти группировки поставили себе на службу социальные сети, чтобы достичь целого ряда целей, таких как координация действий, вербовка сторонников и распространение своей идеологии. При этом они используют социальные сети в качестве виртуального учебного полигона, получая финансовую и моральную поддержку.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Средства ИИ стали лидирующей новой технологией в борьбе с экстремистским контентом в Интернете. Согласно данным «Фейсбук»,, примерно 99% контента Аль-Каиды и ИГИЛ, удаленного с этой платформы, было обнаружено системами ИИ, а не людьми.

Это сделало ИИ лучшим оружием в борьбе с терроризмом в нынешнем мире с огромным объемом информации, поскольку он обладает способностью автоматически обнаруживать контент экстремистского и террористического характера, людей, легко поддающихся обработке со стороны экстремистов и террористов, а также виртуальные сообщества террористов. ИИ оказывает помощь в прогнозировании, предотвращении и уменьшении рисков террористических нападений в будущем.

Нет даже тени сомнения в том, что использование ИИ в антитеррористических программах дает четкие прогнозы, которые приводят к сокращению ненужных действий в отношении большого количества людей, а также снижают фактор человеческой субъективности при принятии решений. ИИ фокусирует свое внимание с большей точностью, сокращая количество подозреваемых, за которыми потребуется дальнейшее наблюдение.

Возможности ИИ прогнозировать события в антитеррористической деятельности уже подтверждены. Службы безопасности и разведки при оценке рисков авиаперелетов и обнаружении связей между террористическими организациями и их сторонниками используют автоматический анализ данных. Некоторые технологические компании используют передовые методы прогнозирования для отслеживания и подрыва террористической деятельности на платформах социальных сетевых ресурсов, а также применяют ИИ для информирования о подозрительных денежных транзакциях в секторе финансовых услуг.

ИИ также используется для анализа социальных сетей, опознания подозрительных пользователей и их взаимоотношений в режиме онлайн, классификации их в соответствии с определенными характеристиками, анализа их коммуникационных отношений и обнаружения в виртуальных общинах тех, кто легко поддается экстремистской обработке. При помощи используемой Агентством национальной безопасности США компьютерной программы SKYNET, в которую включен алгоритм, основанный на ИИ, из 55 млн. пользователей сотовых телефонов внутри страны 15 тыс. были идентифицированы как потенциальные террористы.

«Фейсбук» усовершенствовал свои правила в отношении использования ИИ при удалении экстремистского контента; компания сократила среднее время, необходимое для определения видеосюжета, который нарушает правила использования «Фейсбук» при

прямой трансляции, до 12 секунд.

Еще одним методом удаления радикального контента являются технологии обработки естественного языка, которые потенциально могут повысить эффективность борьбы с контентом экстремистского характера в режиме онлайн. Так считает д-р Маджал бин Султан бин Сафран, преподающий в Университете им. короля Сауда предметы, связанные с искусственным интеллектом.

Эти технологии помогают научить устройства понимать коммуникации человека с ними и обнаруживать информацию в чрезвычайно больших текстовых группах без вмешательства человека и находить отличительные лингвистические модели, характерные для экстремистов и террористов.

ТРУДНОСТИ, СВЯЗАННЫЕ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Несмотря на прогресс, достигнутый в борьбе с контентом экстремистского и террористического характера в Интернете благодаря использованию технологий ИИ, у них есть целый ряд проблем, возникающих при анализе лингвистического контента, особенно с учетом распространения таких гибридных языков как франко, разговорных диалектов, а также при анализе невербальных сигналов и изображений. Из-за этого на цифровой анализ очень большого и сложного контента, который невозможно проверить только человеческими усилиями опытных специалистов, полностью полагаться нельзя.

Нам еще многое предстоит сделать, прежде чем мы разработаем модель, способную уловить истинное и точное значение языкового оборота и выйти за пределы простого запоминания отдельных слов и фраз. Мы должны продвинуться вперед в интерпретировании информации в определенном контексте, которое стало ключевым фактором в понимании поведения пользователей в режиме онлайн.

Клаудия Уоллнер, аналитик в Группе исследований терроризма и конфликтов в Королевском объединенном институте исследований проблем обороны и безопасности, настроена пессимистично в отношении успеха новой стратегии Европейского союза по удалению террористического контента.

Уоллнер считает, что эффективность этой стратегии ограничена несколькими факторами, в том числе и двойственностью понятия контента экстремистского и террористического характера из-за проблем с юридическими определениями. Правительства предлагают изменить определения насильственного экстремизма и терроризма, принимая во внимание то, что в национальные классификационные списки зачастую попадает лишь часть активно действующих экстремистских или террористических группировок.

Обнаружение экстремистского контента представляет собой своеобразную серую зону. Иногда трудно определить, какой контент носит экстремистский характер, а какой нет. В некоторых случаях контент, размещенный экстремистскими группировками или отдельными лицами, не содержит заявлений или намеков, поддерживающих ненависть или насилие, но в нем используются шутки и иронические комментарии, подогревающие чувства озлобленности и недовольства.

К сожалению, борьба с экстремистским контентом в Интернете заставила экстремистов и террористов перейти на более крупные платформы, на которых они могут затеряться среди миллионов вебсайтов, что затрудняет работу правоохранительных органов по обнаружению их деятельности.

Сайты в небольших социальных сетях сейчас более поляризованы, и Аль-Каида, Даиш и другие группировки используют их в своих интересах, поскольку эти платформы не имеют достаточно ресурсов для эффективного отслеживания и удаления террористического контента.

сочетании с использованием промышленных систем управления, инфраструктуры общественных коммуникаций и искусственного интеллекта требуют повышенного внимания к вопросам кибербезопасности на национальном уровне. Кроме того, рост числа новых электронно-физических систем, таких как самоуправляющиеся автомобили, еще больше увеличивает уязвимость.

Также вызывают озабоченность быстрое развитие и взаимозависимость технологий, в основном из-за появления «интернета вещей», который для киберпреступников и террористов создал много новых способов нападения.

8 апреля 2020 г. Агентство по кибербезопасности и безопасности инфраструктуры и Национальный центр по кибербезопасности Великобритании выпустили предупреждение об инцидентах в сфере безопасности, объектами которых были критически важная инфраструктура здравоохранения и фармацевтические компании. В числе жертв нападения оказались компании, медицинские исследовательские институты и университеты, и нападения эти совпали с началом пандемии COVID-19.

В феврале 2021 г. в небольшом городке во Флориде в США хакеры проникли в компьютерную сеть водонапорной станции и попытались поднять уровень потенциально опасных химикатов в поставляемой населению воде. К счастью, это нападение было обнаружено прежде, чем кто-либо пострадал.

В том же месяце Департамент внутренней безопасности США обнаружил вредоносную программу, нацеленную на критически важную инфраструктуру газокомпрессорного предприятия. Злоумышленник с использованием спирфишинга осуществил целенаправленную атаку с намерением обманным путем выведать у людей чувствительную информацию, такую как пароли для получения доступа к сетям учреждений. Из-за этого нападения предприятие пришлось закрыть на два дня.

Поскольку виртуальные нападения становятся все более изощренными, органы, отвечающие за защиту национальной безопасности, в том числе и вооруженные силы, не имеют права ослаблять бдительность. Не в каждом разрушительном нападении на национальный суверенитет используется традиционное оружие. ✦

СЛОВО КАК ОРУЖИЕ

СПОНСИРУЕМЫЙ ИРАНОМ ИСЛАМСКИЙ СОЮЗ РАДИОВЕЩАНИЯ И ТЕЛЕВИДЕНИЯ РАСПРОСТРАНЯЕТ ДЕЗИНФОРМАЦИЮ, ЧТОБЫ ПОДОРВАТЬ СПЛОЧЕННОСТЬ ОБЩЕСТВА

ГЕНЕРАЛ-ЛЕЙТЕНАНТ (В ОТСТАВКЕ) УДА ШУДЕЙФАТ, СОВЕТНИК ПО СМИ И КУЛЬТУРЕ ГЛАВНОЕ КОМАНДОВАНИЕ ВООРУЖЕННЫХ СИЛ ИОРДАНИИ

ИЛЛЮСТРАЦИЯ «UNIPATH»

Новости поступают отовсюду, они сопровождаются анализом, комментариями, общением и обменом мнениями. Основываясь на убеждениях, мнениях и целях СМИ или гостя, программы могут занимать обвинительную, оборонительную или нейтральную позицию по актуальным вопросам.

Во многих передачах рубрики эмоции и способы выражения мнения меняются; терпение истощается, а голоса повышаются, порой даже до крика и ругани, пока зритель не придет в замешательство. Часто бывает трудно уйти от этой мешанины мнений к чему-то реально существующему и полезному. И эта сцена повторяется всякий раз, когда зритель пытается отслеживать свежие новости по разным источникам, обычно по спутниковым каналам.

Мы полностью признаем, что СМИ со всеми их дисциплинированными каналами, изданиями и контентом играют важную роль в современной жизни, и их влияние на нас невозможно приуменьшить. С быстрым развитием информационных технологий и всего, что с ними связано, медиаконтент стал доступен каждому, кто живет теперь в чем-то, напоминающем глобальную деревню.

Однако меня заставляет задуматься наличие армии спутниковых каналов, финансируемых Исламским союзом радио и телевидения, которые транслируют ненавистнические сектантские программы, маскируя уродство вооруженных группировок и называя связанные с ними банды "святыми".

Союз управляет около 210 медиа-компаниями в 35 странах, в основном на Ближнем Востоке. Он включает в себя исследовательские и аналитические центры, группы психологической войны и новостные сайты. Эти учреждения нацелены на определенный сегмент общества, стремясь промывать людям мозги дезинформацией, которая внушает чувство несправедливости и лишений и подталкивает их к восстанию против своих правительств.

На мой взгляд, это явный акт агрессии и объявление войны гражданскому миру арабских обществ. Иран использует эти медиа-щупальца в качестве разменной монеты в отношениях со странами региона и мира, подвергая страны опасности войны и разрушений. В отношении этой организации должны быть введены международные санкции, поскольку она подстрекает к насилию и терроризму точно так же, как Корпус стражей Исламской революции в Иране и органы безопасности.

Можно часто видеть, что в заголовках новостных ток-шоу и тому подобном доминирует определенная тема. В наши дни человек, следящий за новостными сетями в регионе и некоторыми сетями в других странах мира, может не найти ни одной новости или репортажа, в которых не упоминался бы Иран и его режим, цели, задачи, влияние, оружие и воздействие на многие общества, а также его неправомерные действия и вмешательство в другие внутренние и внешние дела стран.

Иран даже манипулирует будущим этих обществ — будущим их детей, их растущими амбициями и их конкретными планами — используя для этого все доступные средства. Например, на уровне глобальных проблем волнует всех и является заметной темой иранская ядерная программа, и информация о ней преследует вас и днем, и ночью. Это уже привело к тому, что некоторые страны региона выделили огромные бюджеты в размере 1,5 млрд. долл. США на борьбу с иранской угрозой.

Малайзия прервала все отношения с Ираном и, совершив беспрецедентный шаг, прекратила все формы сотрудничества с Ираном. Ливан сильно страдает из-за иранского вмешательства. Аналогичным образом, из-за схожего вмешательства переживает ожесточенный конфликт Йемен, в настоящее время вмешательство становится все более заметным в Афганистане. Ситуация в Ираке и Сирии такая же плохая и становится все хуже. Соседние страны Арабского залива и другие страны региона также не застрахованы от аналогичного иранского вмешательства, которое принимает различные формы в зависимости от используемых средств и сил – полевых командиров, игроков, наживающихся на кризисе, и пропагандистов сектантства.

Перед лицом этой интеллектуальной угрозы, поддерживаемой всеми возможными средствами – оружием, боевиками, быстрыми на подъем сторонниками, войной в средствах массовой информации, торговцами наркотиками, экстремистской идеологией и вседозволенностью по отношению ко всему, что служит идеологии страны, охваченной религиозным и национальным фанатизмом, мы не должны бездействовать. Мы должны обеспечить защиту и безопасность наших родных земель, находящихся в эпицентре урагана поддерживаемого Ираном терроризма.

Правительство США заблокировало сайты Исламского союза радио и телевидения, используемые Ираном для пропаганды насильственного экстремизма. РЕЙТЕР

Чтобы остановить стремление Ирана к экспансии за счет стран региона и инвестиций в террористические группировки, нам не нужно объявлять ему войну. Как и другие, я рассматриваю войну как результат неспособности найти политическое решение проблемы. Я призываю всех нас использовать мягкую силу, надеясь при этом, что нас не вынудят защищаться. Это единственный способ обуздать звериные амбиции Ирана. Эта мягкая сила включает в себя экономическое и дипломатическое давление.

Мы должны поддерживать и укреплять региональные и международные партнерские отношения, которые будут сдерживать тех, кто нарушает международное право и прячется за марионетками и наемными убийцами. Иран продолжает свои усилия по приобретению ядерного оружия и представляет опасность для региона еще до того, как он его приобрел. Пусть страна с таким противоречивым поведением обзаведется оружием массового уничтожения, ничего страшного?

Мы должны продолжать оказывать давление на Иран и препятствовать тому, чтобы он поддерживал, укрывал и обучал террористические группы. ✦

БАХРЕЙН СОЗДАЁТ АТМОСФЕРУ ДОВЕРИЯ В ПРОТИВОВЕС

ШИРОКО РАСПРОСТРАНЯЕМОЙ ДЕЗИНФОРМАЦИИ

СТРАНА УСПЕШНО ПОБОРОЛА ПАНДЕМИЮ **COVID-19**, ОПРОВЕРГАЯ РАСПРОСТРАНЯЕМЫЕ В ИНТЕРНЕТЕ СТРАХИ

ХАБИБ ТУМИ, СОВЕТНИК МИНИСТЕРСТВА ИНФОРМАЦИИ БАХРЕЙНА

Во время пандемий, как и во время войн, первой жертвой, похоже, становится правда.

Хотя мир сталкивается с эпидемиями и пандемиями уже не одно столетие, ему никогда еще не приходилось иметь с ними дело в обстановке массированного искажения информации, дезинформации и теорий заговора, которую мы наблюдали при пандемии COVID-19.

Сегодняшнее обилие информации, созданное сочетанием фотографий, голосовых, визуальных и текстовых сообщений, а также сообщений, выдаваемых за факты и легко распространяемых по всем странам, по-новому формирует ракурсы мышления, бросает вызов ожиданиям и сеет растерянность в обществах.

Всемирная организация здравоохранения придумала термин «инфодемия», характеризующий чрезмерное количество вводящей в заблуждение и вызывающей замешательство информации о COVID-19, которая подрывает усилия по сдерживанию распространения вируса, не говоря уже о стремлении остановить его распространение или лечить заболевших.

Переплетение вызывающих страх заболеваний и ложной информации появилось еще во времена первых обрушившихся на людей потрясений, и люди в течение веков приписывали это колдовским чарам, сглазу, злому умыслу дьявола или мести разгневанных богов.

ИЛЛЮСТРАЦИЯ «UNIPATH»

Пока болезни поражали свои жертвы, ложная информация нацеливалась на предполагаемых виновников этих бед, что приводило к их казни, изоляции или изгнанию.

Эти обвинения придумывались в соответствии с политическими, экономическими и социальными обстоятельствами и были нацелены на евреев, христиан, мусульман, женщин, африканцев, азиатов, представителей меньшинств, прокаженных, нищих, бродяг и иностранцев. У тех, кто придумывал эти истории, обвинения и слухи, похоже, никогда не было недостатка в дезинформации.

Независимо от исторического периода, цели распространения ложной информации и дезинформации всегда оставались одними и теми же, только сами нарративы видоизменялись в зависимости от особенностей конкретной вспышки заболевания.

В своей книге «Эпидемия слухов», вышедшей в 2014 г., ее автор Джон Ли пишет, что «нарративы кочуют от одной эпидемии к другой, и изменения претерпевает не сама тематика, а отдельные детали, необходимые для привязывания нарративов к текущей ситуации».

Отдельные «отредактированные» фотографии и ложные нарративы появляются в результате злого умысла, процветающего в периоды кризисов, страха и тревоги, другие же являются следствием нездорового желания потешится или ненормального понимания, что считать забавой.

Благодаря современным технологиям искажение фактов и придумывание историй стало простым и эффективным занятием. Онлайновые приложения дали людям возможность создавать выдуманный мир, заменяющий реальный и отодвигающий на второй план факты. Качественный технологический прорыв, который, как предполагалось, должен был улучшить жизнь людей, вместо этого используется во зло.

В первые дни 2020 г., когда мир узнал о COVID-19, людей просто забрасывали сообщениями из их ближайшего круга общения – от родственников, друзей, коллег, соседей – и из внешних источников информации, таких как врачи, эксперты в сфере здравоохранения, знаменитости, правительственные чиновники и политические деятели.

Руководители большинства стран понимали, что существенным компонентом стратегии борьбы с повальным заболеванием должно стать противостояние снежному кому ложной информации, способной до получения вакцины подорвать усилия по сдерживанию пандемии.

Бахрейн, небольшое островное государство (площадью 765 квадратных километров) с одной из самых высоких в мире плотностью населения (примерно 2 тыс. 52 человека на квадратный километр), оказался в числе стран с высоким риском заражения. При этом «заражение» людей через Интернет и социальные сетевые ресурсы может быть не менее опасным.

По данным организации DataReportal, в январе 2020 г. охват Интернетом в Бахрейне находился на

Люди стоят в очереди на вакцинацию от COVID-19 в торговом центре «Ситра» в Манаме. Несмотря на эффективные меры, принимаемые Бахрейном по сдерживанию распространения заболевания, злоумышленники распространяют в стране дезинформацию о пандемии. РЕЙТЕР

уровне 99%, а охват социальными сетевыми ресурсами составлял 84%. В то же время в стране было 1,65 млн. пользователей Интернета и 1,4 млн. пользователей социальных сетевых ресурсов.

Национальная межминистерская рабочая группа, созданная в начале февраля 2020 г. для сдерживания распространения и борьбы с последствиями пандемии, имела внушительный медийный составной элемент. Одновременно с противостоянием пандемии правительство встало на борьбу с ложной информацией и дезинформацией, при помощи которой высокий уровень пользования населения цифровыми платформами использовался для подрыва усилий государства.

Рабочая группа призывала людей пользоваться только вызывающими доверие источниками информации и не становиться жертвами ложных и вводящих в заблуждение заявлений различных искателей славы, распространителей теорий заговора и хвастунов.

Для оперативных коммуникаций рабочая группа открыла «горячую линию» на семи языках, ведь более половины населения Бахрейна в 1,7 млн. человек составляют жители, приехавшие из более чем 140 стран.

В Бахрейне издаются четыре ежедневные газеты на арабском языке, две на английском, одна на малаялам-ском (для индийцев) и одна на тагалогском (для филиппинцев) языках. Еженедельные и ежемесячные журналы выпускаются на нескольких языках, так же, как и радио и телевизионные передачи.

Они все осознали серьезность ситуации и строго придерживались правила печатать и транслировать новости и сообщения, полученные только из заслуживающих доверия источников, таких как выступления официальных представителей, заявления экспертов и полицейских и объявления, сделанные министерствами.

СМИ категорически отказались иметь дело с сомнительными заявлениями и часто направляли репортеров для бесед с медицинскими экспертами, главным образом с консультантами в области инфекционных и внутренних заболеваний и микробиологами, которые давали

научные объяснения, помогая людям разобраться в ситуации. Они оказали огромную помощь в опровержении ложной информации.

Религиозные деятели в своих проповедях и речах приравнивали распространение лжи к нарушению религиозных учений и ценностей.

Также органы безопасности и правопорядка регулярно выпускали предупреждения о том, что тем, кто распространяет фальшивую информацию, будет предъявлено обвинение в нарушении общественного спокойствия, за которым последует наказание в виде тюремного заключения и крупных штрафов.

Рабочая группа регулярно проводила пресс-конференции, на которых давала обновленную информацию и разъяснения по отдельным вопросам, а также призывала граждан к глубокому чувству ответственности, напоминая всем о негативных последствиях распространения слухов и домыслов.

Высокий уровень грамотности среди взрослого населения (97,5% в 2018 г.) и кампания под названием «Будь осторожен!» внесли существенный вклад в формирование атмосферы доверия между населением и государственными и частными институтами, что помогло остановить распространение различных теорий заговора, которыми изобилует регион Ближнего Востока.

В целом, противостояние ложной информации и дезинформации в Бахрейне стало сочетанием оперативных действий рабочей группы, жестких предупреждений нарушителям и открытого общения между медицинскими экспертами и ответственными журналистами.

Большое количество ложной информации и дезинформации доходило до людей в Бахрейне через приложение «WhatsApp», наиболее часто используемое в стране для коммуникаций.

Премьер-министр Бахрейна, Его Королевское Высочество наследный принц Салман бин Хамад Аль Калифа получает бустерную прививку от COVID-19. МИНИСТЕРСТВО ИНФОРМАЦИИ БАХРЕЙНА

Бахрейн призывает общественных деятелей координировать меры государства по сдерживанию распространения вируса COVID-19. РЕЙТЕР

В основном эти сообщения не были привязаны к политическим, религиозным и межэтническим аспектам, которые, к сожалению, доминируют на Ближнем Востоке из-за противостояния между различными объединениями верующих и государствами.

Наиболее беспокоящие сообщения появились 26 февраля, через два дня после того, как был зарегистрирован первый случай инфекции у гражданина Бахрейна, вернувшегося из Ирана, где он находился по религиозным причинам. В сообщениях в приложении «WhatsApp» критиковались граждане Бахрейна, которые ездили в Иран, обвиняя их в том, что они завозят в страну болезнь и подвергают жителей Бахрейна опасности. Источники в полиции утверждают, что 30 аккаунтов содержали сообщения с межэтнической направленностью.

Однако, оперативное вмешательство Его Королевского Высочества наследного принца Салмана бин Хамада Аль Калифы помогло снизить вызванную страхом напряженность. Он призвал к сохранению единства и отметил, что «COVID-19 поражает всех людей, независимо от их расовой, этнической и религиозной принадлежности и социального статуса».

Другие попытки дезинформации были направлены на обман пользователей или стремление повлиять на их поведение. Вот несколько примеров такой дезинформации:

- В социальных сетевых ресурсах появилось сообщение о том, что случаи инфицирования COVID-19 были зарегистрированы в «Городе дракона», огромном торговом центре с китайской тематикой, и что полиция провела там рейды в магазинах, торгующих аксессуарами, предметами внутреннего убранства домов и продуктами питания.
- В другом случае, в социальных сетевых ресурсах циркулировало сообщение о том, что из карантинного центра сбежали зараженные COVID-19 люди и рассеялись по всей стране. В обоих случаях полиция быстро дала опровержение.
- Один пользователь был задержан полицией после того, как в своем посте он поместил утверждение о том, что COVID-19 является большим «фейком» с целью отъема у людей побольше денег.
- Известная певица нажила себе неприятности с законом после того, как через «WhatsApp» предостерегала людей о том, что пицца и другие продукты, доставляемые на дом, содержат опасные инфекции.
- Утверждение, что несколько заключенных в тюрьме инфицированы коронавирусом, что было опровергнуто Национальным институтом прав человека в отчете, составленном после посещения тюрьмы.
- Другая дезинформация, циркулировавшая в стране, ссылалась на «достоверные» или «секретные» сообщения о происхождении вируса и о способах лечения новой вирусной инфекции.

Сегодня, спустя два года после вспышки заболевания, Бахрейн занимает первую позицию в «Индексе выздоровления от COVID-19 на ноябрь 2021 г.», составленном компанией «Nikkei». Королевство продолжает прилагать огромные усилия по борьбе с пандемией и возвращению к нормальной жизни.

Бахрейнцы приветствуют гостей из Саудовской Аравии после того, как страна открыла в 2021 г. свои границы для вакцинированных от COVID-19. РЕЙТЕР

Этот индекс, впервые опубликованный в июле 2021 г., оценивает процесс выздоровления населения от коронавируса в 121 стране, беря за основу девять показателей, объединенных в три категории: сдерживание распространения инфекции, вакцинирование населения и мобильность.

Меры сдерживания предусматривают такие показатели как число подтвержденных случаев заболевания по сравнению с количеством случаев в пиковый период, количество подтвержденных случаев на душу населения и количество тестов на каждый случай.

Прогресс в вакцинировании учитывает такие показатели как количество имеющихся доз на душу населения, число вакцинированных на душу населения и процент полностью вакцинированных жителей страны.

Категория мобильности рассматривает мобильность населения, оксфордский индекс строгости принимаемых мер и воздушные передвижения людей.

Выставляются баллы от 0 до 90, и чем выше у страны балл, тем ближе она находится к рубежу выздоровления с низким числом случаев заболевания, тем больше у нее процент вакцинированных и менее строгие правила социального дистанцирования. Показатель Бахрейна – 73%, за ним идут Кувейт с 72% и Объединенные Арабские Эмираты с 70,5%.

В ноябре 2021 г. регулирующий орган здравоохранения Бахрейна одобрил применение в чрезвычайных случаях вакцины «Pfizer» и «BioNTech» для детей в возрасте от 5 до 11 лет. Это решение последовало за оценкой свойств этой вакцины, проведенной Комитетом клинических исследований Национального регулирующего агентства здравоохранения и Комитетом по вакцинации Министерства здравоохранения. ✦

ПРИВЕРЖЕННОСТЬ КИБЕРБЕЗОПАСНОСТИ

Защита Ирака от киберугроз требует формирования национальных кадров, специализирующихся на информационных технологиях

Д-Р ХУССЕЙН АЛЛАВИ, СОВЕТНИК ПРЕМЬЕР-МИНИСТРА ИРАКА ПО ВОПРОСАМ РЕФОРМ СЕКТОРА БЕЗОПАСНОСТИ

Кибербезопасность является стратегическим приоритетом для правительства Ирака. Была создана группа реагирования на киберинциденты (CERT), принята политика кибербезопасности, и после длительного обсуждения в иракском парламенте был одобрен закон о преступлениях в электронной сфере.

Основная задача CERT состоит в том, чтобы противостоять кибератакам во всех министерствах, сотрудничать с органами безопасности и разведки, отслеживая хакеров и террористические группировки и преследуя банды киберпреступников. Такие меры предосторожности необходимы в современных обществах, таких как иракское, которые все больше полагаются на услуги интернета при переводе денег и функционировании правительственных учреждений.

ИЛЛЮСТРАЦИЯ «UNIPATH»

Кибератаки представляют собой возрастающую угрозу для всего мира и заставляют международное сообщество выражать беспокойство относительно того, что террористические группировки получают доступ к передовым технологиям для осуществления кибернападений на жизненно важные объекты.

Учитывая все это, в сентябре 2021 г. Ирак организовал в Багдаде вторую Национальную конференцию по вопросам создания и развития потенциала безопасности в киберпространстве. Эта конференция представляла собой большой сдвиг в работе иракского CERT. На конференции рассматривались такие беспокоящие всех вопросы как преступления в электронной среде, киберозможности противостояния войнам, связанным с 5G, влияние кибербезопасности и современных технологий на национальную безопасность и защита детей, пользующихся интернетом. В числе других тем были влияние кибербезопасности на людей в мире, оказавшемся в осаде дезинформации, цифровая безопасность для студентов и отмывание денег и финансовые транзакции в режиме онлайн.

Конференция также включала техническую демонстрацию, проведенную иракской CERT, венцом которой стало упражнение по защите кибербезопасности, в ходе которого группа специалистов быстро вмешалась и отразила киберугрозу.

Глава иракской CERT Атир Аль-Джаббер подчеркнул важность конференции в свете принятия компаниями и правительством страны электронной автоматизации, вызванной COVID-19.

«На различных этапах этой конференции мы сделали еще один шаг вперед к успешному предоставлению услуг в киберпространстве», - подчеркнул Аль-Джабер.

Обмен техническими знаниями, приобретенными дружественными странами в процессе отражения кибератак или восстановления сетей после взлома систем безопасности, считается основой кибербезопасности. Ирак использует в своих целях опыт дружественных стран в технологической сфере и создает и развивает собственные возможности обеспечения безопасности в киберпространстве.

Со своей стороны, Ирак готов делиться полученной информацией относительно того, как террористы используют в своих интересах кибертехнологии для коммуникаций, шифрования и планирования нападений. Поскольку террористические группы и организованные преступные группировки обмениваются своими идеями и технологиями, международное сообщество должно объединить усилия и сорвать их преступные планы.

Основой кибербезопасности является создание сектора передовых технологий, имеющего достаточно ресурсов для отражения изощренных кибернападений. Ирак должен постоянно пересматривать национальные правила кибербезопасности и повышать свои возможности. Правительство Ирака старается привлечь энергичных людей в сектор безопасности и на государственную службу с целью развития потенциала страны в области кибербезопасности и сотрудничества с участием правительственных кругов, частного сектора и международных компаний.

Ирак стремится воспитать единую культуру, которая бы противостояла киберугрозам, снижала количество случаев похищения и незаконного опубликования информации, останавливала распространение дезинформации, угрожающей гражданскому миру, и снижала число киберпреступлений, совершаемых бесчестными субъектами в отношении пользователей интернета.

Партнерство между общественным и частным секторами, в том числе и в вопросах кибербезопасности, является стратегически необходимым. Такие отрасли как здравоохранение, образование и энергетика в своей работе все больше зависят от компьютерных сетей.

Именно поэтому правительство Ирака и группа CERT готовы предлагать новые решения в сфере информационных технологий. Правительственные министерства используют финансовые стимулы для поощрения энтузиастов в области информационных технологий и кибербезопасности. Ирак также должен сосредоточить внимание на том, чтобы женщины вносили больший вклад в эту важную деятельность. Они будущая сила нашего процветающего общества, которое сталкивается с многочисленными проблемами.

Предоставление женщинам новых возможностей является чрезвычайно важной частью программы и философии занятости иракского правительства. В развитых странах женщины играют выдающуюся роль в развитии технических областей, и технологический прогресс во многом обязан женщинам, работающим в таких чувствительных сферах как социальные СМИ, индустрия компьютерного программирования и электронный маркетинг.

Сегодня мы должны оказывать поддержку стремительному развитию бизнеса и электронной торговли, а также инвестициям в информационные технологии во всех регионах Ирака. Для этого мы должны совершенствовать законодательную базу и общественные правила, а также создавать условия для соответствия требованиям кибербезопасности. Мы должны поддерживать планы иракского правительства по созданию партнерских отношений между Ираком и международным бизнес-сообществом, создавая благоприятную обстановку для роста компаний в секторе информационных технологий, что будет служить на благо общества и модернизировать его возможности.

К счастью, правительству Ирака удалось успешно оказать поддержку Независимой высшей избирательной комиссии в проведении свободных и честных выборов и в ее противостоянии кибератакам во время парламентских выборов 10 октября 2021 г., что стало убедительным подтверждением возросших способностей Ирака бороться с кибернападениями и укреплять системы кибербезопасности. ✦

КАЗАХСТАН ВОЗВОДИТ КИБЕРЩИТ

Программа Казахстана делает упор на защиту систем от хакеров и преступников

САЛТАНАТ БЕРДИКЕЕВА

ИЛЛЮСТРАЦИЯ «UNIPATH»

Более 85% населения Казахстана пользуется Интернетом, что является самым высоким показателем среди стран Центральной Азии. Основные сегменты экономики и правительство страны уже переведены на цифровые платформы. В 2018 г. правительство Казахстана приступило к осуществлению программы «Цифровой Казахстан», стимулирующей переход правительственных учреждений и частных компаний с традиционного физического доступа на онлайновый доступ для более эффективного обслуживания клиентов.

Вместе с тем, крупномасштабный переход Казахстана на цифровую экономику привел к необходимости значительно повысить уровень кибербезопасности, особенно после начала пандемии COVID-19, которая заставила многих людей работать и учиться удаленно.

Это подтолкнуло власти Казахстана к введению серьезных мер противодействия киберугрозам. Несмотря на то, что в борьбе с киберпреступлениями имеются трудности, и интенсивность, масштабы и изощренность таких преступлений постоянно возрастают, результаты усилий Казахстана по борьбе с преступлениями и угрозами в киберпространстве за последние годы были довольно существенными.

Благодаря недавним усовершенствованиям в сфере кибербезопасности, в «Глобальном индексе кибербезопасности – 2020», выпущенном Международным союзом телекоммуникаций, являющимся инициативой ООН в области информационных и коммуникационных технологий, Казахстан оказался на 31 месте из 182 стран.

Этот индекс основывается на пяти основных факторах: юридические, технические и организационные аспекты, а также развитие имеющихся возможностей и принятие коллективных мер. В 2020 г. Казахстан занял гораздо более высокое место по сравнению с 83-м местом в «Глобальном индексе кибербезопасности – 2017».

УСТАНАВЛИВАЯ КИБЕРЩИТ

Политика Казахстана в сфере кибербезопасности берет свое начало с программы «Киберщит Казахстана», принятой в 2013 г. Нурсултаном Назарбаевым, бывшим в то время президентом страны. Он тогда подчеркнул, что разработка стратегии кибербезопасности отвечает национальным интересам Казахстана, указывая на способность преступников отключить некоторые объекты инфраструктуры, такие как электростанции или движение поездов.

«В сегодняшнем мире для ведения войны уже не обязательно использовать самолеты и танки», - отметил Назарбаев в 2017 г. В том же году Казахстан разработал государственную политику, указывающую, как предотвращать, сдерживать и отражать кибератаки и гибридные нападения, а также предписывающую усовершенствовать законодательную базу страны, чтобы сделать эти усилия более эффективными. При принятии этой концепции казахские власти

Превращение Казахстана в страну передовых цифровых технологий требует особого внимания к вопросам кибербезопасности. Вид на столицу страны г. Астана, являющийся центром технологических инноваций. АССОШИЭЙТЕД ПРЕСС

проконсультировались с международными экспертами и взяли на вооружение самый передовой опыт в сфере кибербезопасности. Первый этап программы «Киберщит» проходил в 2017-2018 гг., а второй длился с 2019 г. по 2020 г. На сегодняшний день на программу было потрачено 28 млрд. казахских тенге (примерно 66 млн. долл. США).

Министерство цифрового развития, инноваций и аэрокосмической промышленности Казахстана стало основным правительственным учреждением, ответственным за реализацию плана действий «Киберщит» в сотрудничестве с совместным предприятием «Государственная техническая служба», которое в настоящее время входит в Министерство инвестиций и развития Казахстана.

Программа «Киберщит» определяет государственную политику в таких сферах как защита электронных информационных ресурсов, информационных систем и телекоммуникационных сетей, а также обеспечивает безопасное использование информационных и коммуникационных технологий. Эта концепция помогла унифицировать все предыдущие кустарные подходы к обеспечению кибербезопасности. Программа «Киберщит» также предполагала создание механизмов экстренного реагирования в целях предотвращения инцидентов в сфере информационной безопасности, в том числе и во время чрезвычайных ситуаций.

ПРЕСТУПНИКИ НАЦЕЛИЛИСЬ НА КАЗАХСТАН

Весной 2021 г. базирующийся в Великобритании вебсайт Comparitech, занимающийся оценкой технологий и потребительских товаров, выпустил доклад, в котором назвал наиболее и наименее безопасные страны в плане возможных кибернападений. В нем страны Центральной Азии, включая Казахстан, находятся почти в конце списка.

Казахстан является одной из наиболее привлекательных стран для т.н. «криптоугонщиков», создающих

цифровую валюту, или криптовалюту, получая доступ к уязвимым компьютерам. Этот процесс называется добычей криптовалюты, или криптодобычей. Не получая разрешения владельцев компьютеров, «криптоугонщики» избегают оплаты огромных объемов электроэнергии, необходимых для криптодобычи. Казахстан привлекает криптодобытчиков своими низкими ценами на электроэнергию и низким уровнем компьютерной безопасности по сравнению с другими странами мира.

Одна из основных причин, почему компьютерные сети в стране менее защищены, состоит в том, что почти 74% программного обеспечения, установленного на компьютерах в Казахстане, было нелицензированным или установлено из незаконных источников. Об этом говорилось на встрече рабочей группы казахских экспертов по программному обеспечению в 2019 г.

Нелицензированное программное обеспечение может содержать вредоносные программы, способные угрожать компьютерным данным пользователя, и для такого программного обеспечения трудно устанавливать обновления механизмов защиты от кибернападений. В результате компьютеры с пиратским программным обеспечением чрезвычайно уязвимы для хакерских атак, криптодобычи, краж конфиденциальной информации, мошенничества и других форм киберпреступлений.

«Количество киберугроз правительственным учреждениям Казахстана удваивается каждый год», - отметил в 2017 г. в своем заявлении председатель Комитета информационной безопасности бывшего Министерства обороны и аэрокосмической промышленности Руслан Абдикаликов.

В первой половине 2021 г. Казахстанская государственная Служба реагирования на компьютерные инциденты, известная как KZ-CERT, зарегистрировала 11 тыс. 432 киберпреступления и угрозы информационной безопасности, что на 15% больше чем в 2020 г. По данным KZ-CERT, наиболее распространенным вредоносным программным обеспечением, используемым киберпреступниками для нападения на компьютерные сети в Казахстане, являются ботнеты, вредоносные программы «Троянский конь» и компьютерные вирусы.

Кибератаки на модули управления контентом WordPress (программное обеспечение, используемое для создания веб-сайтов и контента, публикуемого в Интернете), широко распространенные в Казахстане, для многих пользователей закончились потерей конфиденциальной и чувствительной информации и показом террористических и экстремистских пропагандистских посланий на взломанных сайтах.

С целью получения финансовой выгоды киберпреступники постоянно атакуют казахские частные компании, государственные учреждения и отдельных граждан. В августе 2021 г. ни один казахский банк не смог продемонстрировать способность защитить от кибератак свои веб-ресурсы, в том числе обеспечить безопасность контента, передачи данных, шифрования трафика и настройки механизма безопасности.

ОТРАЖЕНИЕ КИБЕРАТАК

Принимая во внимание тот факт, что, в соответствии с данными генерального директора Сити Банк Казахстана Андрея Курилина, кибернападения на основные международные банки происходят каждую секунду, слабая киберзащищенность казахских банков вызывает особую озабоченность.

И, тем не менее, после принятия концепции «Киберщит» в 2017 г. возросшие усилия правительства Казахстана по мониторингу киберпространства и принятию инициативных мер существенно снизили уровень киберугрозы. К 2019 г. Министерство цифрового развития, инноваций и аэрокосмической промышленности уже имело достаточно знаний об источниках и временных рамках кибератак на сети Казахстана. Министерство помогло снизить количество взломанных веб-сайтов и зараженных программ в стране.

Благодаря программе «Киберщит» более 300 объектов критической инфраструктуры, включая банки, правительственные учреждения, частные компании и производственные предприятия, повысили уровень безопасности своих систем. Государственная техническая служба Казахстана создала достаточно возможностей для сдерживания и предотвращения почти одного миллиона кибератак в день.

В 2018 г. Комитет национальной безопасности Казахстана создал Национальный координационный центр информационной безопасности (НКЦИБ), призванный защищать от кибернападений информационные ресурсы государственных учреждений и критическую информационную инфраструктуру Казахстана. В 2020 г. НКЦИБ предоставил 17 правительственным ведомствам средства антивирусной защиты и мониторинга их информационных систем на предмет выявления киберинцидентов и угроз.

Одной из ключевых частей программы «Киберщит» является обучение специалистов в сфере кибербезопасности и разъяснение общественности важности информационной безопасности. Из-за нехватки в Казахстане обученных специалистов в области информационных технологий власти стали назначать специальные стипендии студентам университетов, которые продолжат обучение по специальности кибертехнологий. Перед Министерством цифрового развития, инноваций и аэрокосмической промышленности была поставлена задача организовать обучающие и образовательные мероприятия для всего населения страны.

В рамках плана действий по программе «Киберщит» впервые в истории Казахстана правительство страны ввело добровольное киберстрахование, позволяющее юридическому лицу получить финансовую компенсацию за имущество, поврежденное в результате кибератаки или утечки данных.

Власти Казахстана отмечают, что население в большинстве своем остается слабо информированным об основных угрозах кибербезопасности, таких как риск случайно загрузить вредоносную программу, что может привести к фишингу или мошенничеству в режиме онлайн.

Жители Казахстана, как этот мужчина на избирательном участке (2019 г.), все шире используют технологии на основе смартфонов, что вызывает озабоченность по поводу кибербезопасности.
AFP/GETTY IMAGES

ВАЖНОСТЬ ОБРАЗОВАНИЯ

Власти осознают, что быстрый переход страны к цифровой модели экономики и управления требует более высокого уровня вовлеченности общественности и её информированности об аспектах компьютерной безопасности для того, чтобы снизить количество кибернападений и сопутствующего ущерба. Власти Казахстана отмечают, что население в большинстве своем остается слабо информированным об основных угрозах кибербезопасности, таких как риск случайно загрузить вредоносную программу, что может привести к фишингу или мошенничеству в режиме онлайн.

Более того, многие компании малого и среднего бизнеса в стране не имеют даже базовых знаний о защите информации и коммуникационных технологий.

Именно поэтому государство основной упор сейчас делает на повышении общественной информированности и проведении образовательных кампаний для того, чтобы дать людям основные инструменты для защиты компьютеров и коммуникационных технологий. Согласно недавнему опросу, эти усилия были эффективными и обеспечили повышение общественной информированности об угрозах кибербезопасности, поскольку об этих угрозах сейчас знают 78% опрошенных.

Казахстан также инвестирует в обучение госслужащих по вопросам кибербезопасности, законодательства в области информационных технологий, а также «электронного правительства». С 5 января 2021 г. Академия общественной администрации при президенте Казахстана организовала онлайновые курсы для обучения госслужащих в сфере перехода правительственных учреждений на цифровые платформы. В 2019 г. Министерство цифрового развития, инноваций и аэрокосмической промышленности провело с правительственными чиновниками из более чем 20 госучреждений и 17 местных правительственных ведомств бесплатные онлайновые учебные курсы по аспектам кибербезопасности.

В начале глобальной пандемии в 2020 г. многие правительственные чиновники в Казахстане перешли на удаленный режим работы. В целях усовершенствования навыков работы с цифровыми и коммуникационными технологиями у казахских госчиновников Академия общественной администрации, казахское отделение Программы развития ООН, Центр государственной службы в Астане и Агентство по делам государственной службы организовали в 2020 г. широкомасштабное обучение государственных сотрудников.

В своем обращении к нации 1 сентября 2021 г. президент Кассым-Жомарт Токаев отметил, что «все информационные и технологические инициативы общественного сектора в Казахстане будут базироваться исключительно на новой платформе под техническим надзором государства. Это позволит исключить дублирование, сократит стоимость и устранит бюрократические проволочки, и все общественные услуги будут предоставляться гражданам на 100% через их смартфоны».

Дальнейший переход государственных услуг на цифровые платформы потребует инвестиций в обучение государственных служащих азам кибербезопасности. Видение президента Токаева цифрового Казахстана, в котором почти все государственные услуги будут предоставляться электронным путем, и частный сектор будет использовать электронную торговлю, неотъемлемо от его обязательств по постоянному укреплению кибербезопасности в стране. ✦

КАТАР

ВОЗГЛАВИЛ УСИЛИЯ СОЮЗНИКОВ ПО СПАСЕНИЮ ДЕСЯТКОВ ТЫСЯЧ АФГАНЦЕВ

ИЛЛЮСТРАЦИЯ «UNIPATH»

Корреспондент журнала «Unipath», издаваемого Центральным командованием США, взял интервью у начальника Управления международного военного сотрудничества Вооруженных силы Катара штабного генерал-майора Абдулазиза Салеха Аль Сулаити, который был свидетелем операции по эвакуации афганцев и исторической гуманитарной роли руководства Катара в соответствии с указаниями Его Высочества эмира Катара шейха Тамима бин Хамада Аль Тани. Катар оперативно отреагировал, эвакуировав и предоставив убежище десяткам тысяч афганцев и граждан других стран, вынужденных покинуть Афганистан в условиях чрезвычайно сложной ситуации безопасности, сложившейся в августе 2021 г.

Штабной генерал-майор Абдулазиз Салех Аль Сулаити

«Unipath»: Как основное должностное лицо, отвечавшее за проведение операции по эвакуации афганцев, ставшей одной из крупнейших логистических операций за последнее время, могли бы Вы рассказать о том, как все началось и каковы были обстоятельства и детали операции?

Генерал-майор Сулаити: После того, как силы коалиции получили приказ выйти из Афганистана, ситуация стала нестабильной. Кампания по эвакуации основывалась на гуманитарных соображениях, а также на национальной, региональной и глобальной роли политического и военного руководства Катара, являющегося частью международного сообщества. Усилия также координировались с нашим стратегическим союзником, Соединенными Штатами. В ответ на указания Его Высочества эмира Катара шейха Тамима бин Хамада Аль Тани относительно предоставления всевозможной поддержки и помощи власти страны предпринимали соответствующие меры. Это дало быстрый и позитивный результат при проведении самой крупной и самой оперативной операции по эвакуации людей в современной истории.

«Unipath»: Каким образом Вы получили распоряжение начать операцию по эвакуации?

Генерал-майор Аль Сулаити: Министерство иностранных дел Катара передало нам запрос Центрального командования США, в котором говорилось о предстоящем прибытии группы людей из Афганистана. В соответствии с приказом министерства, мы начали предпринимать соответствующие усилия. Поначалу поступило распоряжение эвакуировать из Афганистана в течение года граждан Катара общей численностью примерно 8 тыс. человек. Поэтому были подготовлены лагеря Аль Удеид и Ас Сайлия, согласованы рабочие механизмы и механизмы транспортировки с тем, чтобы все прибывающие имели штриховое кодирование и разрешение на выезд из Афганистана. Учитывая ситуацию с COVID-19, мы приняли предполетные меры предосторожности. Операции были хорошо организованы, однако после того как люди беспорядочно стали пытаться вскарабкаться на готовый к отлету из Афганистана американский самолет, приказы поменялись.

«Unipath»: Как вы сотрудничали с Центральным командованием и реагировали на его просьбы?

Генерал-майор Аль Сулаити: От государственного министра по делам обороны мы получили прямое указание оказать США всестороннюю поддержку, которая не ограничивалась только нашими вооруженными силами. Это были совместные усилия Министерства иностранных дел Катара, госдепартамента США, Вооруженных сил Катара, Фонда развития Катара и Министерства здравоохранения Катара. Госпиталь Аль-Вакра, самый большой и один из самых лучших госпиталей в Катаре, был оборудован всем необходимым для приема и обслуживания беженцев-пациентов.

«Unipath»: Какие трудности при проведении эвакуации оказались самыми серьезными?

Генерал-майор Аль Сулаити: Транспортировка пациентов в другие госпитали оказалась затруднительной; некоторые пациенты прибыли без легального разрешения или без удостоверяющих личность документов, другим требовались дополнительные услуги. События развивались стремительно, что создавало определенные трудности, однако Его Высочество эмир Катара шейх Тамим бин Хамад Аль Тани лично распорядился, чтобы госпиталь Аль-Вакра был полностью отведен под обслуживание беженцев, нуждавшихся в медицинской помощи.

Афганским беженцам были предоставлены раскладушки на базе Аль Удеид в Катаре. РЕЙТЕР

«Unipath»: Существовало несколько маршрутов проведения операции по эвакуации. Что Вы можете о них сказать?

Генерал-лейтенант Аль Сулаити: Для операций по эвакуации мы установили четыре маршрута. Первый маршрут был для дипломатов, и он не представлял особых сложностей, поскольку дипломаты прибывали с членами своих семей, и некоторые из них оставались в стране, а другие продолжали путь к конечному пункту назначения. Второй маршрут был для журналистов, студентов и людей из других стран, попросивших Министерство иностранных дел эвакуировать определенных людей. Эту группу беженцев размещали в специально подготовленных для них лагерях. Третий маршрут был для таких стран как Индия и Бангладеш, которые попросили разрешения эвакуировать своих граждан через аэропорты Катара, используя собственные самолеты.

По четвертому маршруту летали самолеты С-17 Центрального командования США. С этим маршрутом были связаны сложности из-за огромного количества людей, стремившихся покинуть Афганистан, и из-за возрастающей угрозы вокруг кабульского аэропорта. Еще более трудной делало ситуацию то, что люди, собравшиеся вокруг аэропорта, имели различные проблемы со здоровьем, которые становились все серьезнее. Мы были свидетелями того, как американские военнослужащие на руках переносили детей через высокие ограждения. Из-за сильного столпотворения, для этих детей это был вопрос жизни и смерти, и когда они прибывали в Катар, мы делали все возможное, чтобы после распределения по возрастным категориям разместить их в нашем Центре попечения сирот. У нас возник ряд трудностей при обработке паспортов; для людей Катар был промежуточным пунктом перед дальнейшим следованием в конечный пункт назначения, и поэтому возникали сложности с их въездом в нашу страну.
Мы уже готовились проводить Чемпионат арабских стран по футболу как прелюдию к Чемпионату мира.

Одновременно с этим нас удивили происходящие события и скорость, с какой они разворачивались, особенно, когда некоторые страны отказались принять этих людей или задерживали их прибытие. С целью снизить количество людей, ожидавших эвакуации, транспортные самолеты С-17 ВВС эмира Катара осуществили несколько полетов с базы Аль Удеид на военные базы под командованием США и их союзников.

«Unipath»: Как вы координировали выполнение задания с Центральным командованием?

Генерал-майор Аль Сулаити: Первоначальное соглашение с Центральным командованием предусматривало принятие Катаром 8 тыс. беженцев в течение года, поэтому мы были удивлены, когда в ту первую неделю прибыло 16 тыс. человек. У нас были приказы от начальника штаба и министра обороны относительно создания временных лагерей с оборудованием для охлаждения воздуха и всем другим необходимым. На выполнение этой задачи нам отвели три дня, и мы очень торопились с созданием этих лагерей. За эти три дня количество беженцев сначала удвоилось и достигло 30 тыс., потом возросло до 40 тыс., затем до 50 тыс. Основная проблема состояла в том, что беженцы прибывали в августе, когда температура воздуха становится довольно высокой, и поэтому мы старались разместить их в прохладных местах. С другой стороны, для того, чтобы при въезде в страну правильно и организованно выполнить все формальности, все группы прибывших должны были собираться в одном месте.

У нас возникали трудности даже с самыми обычными вещами. Например, большое скопление людей затрудняло соблюдение санитарных и других мер, что побудило Министерство муниципального строительства вмешаться и оказать помощь. Мы приняли все необходимые меры и удвоили наши усилия. Что касается продуктов питания, то беженцам раздавали уже готовую еду, а мы на терминале аэропорта Аль Удеид открыли оперативный центр. Центром руководила поверенная в делах США в Катаре посол Грета Хольтц, специально прибывшая для руководства операцией по эвакуации и предоставлению убежища афганским беженцам.
Со стороны Катара были задействованы сотрудники Министерства иностранных дел, Управления международного военного сотрудничества Вооруженных силы Катара, логистических и медицинских служб, а также Министерство внутренних дел, Таможенная служба, Министерство здравоохранения, Служба скорой помощи и Благотворительная служба Катара. В задней части терминала работала отдельная группа из военных.
Эту группу возглавлял руководитель оперативного отдела Мухаммед Хамад Аль-Нуаими. Сотрудники Министерства здравоохранения стали оказывать поддержку этой группе. Желающих эвакуироваться было очень много, а время было ограничено, и поэтому мы были удивлены тем, что самолеты только доставляли беженцев, но никого не эвакуировали в другие страны,

ВО ВРЕМЯ КРИЗИСНЫХ СИТУАЦИЙ, ОСОБЕННО ВО ВРЕМЯ ГУМАНИТАРНЫХ КРИЗИСОВ, РОЛЬ СОЮЗНИКОВ ЗАКЛЮЧАЕТСЯ В СОВМЕСТНОМ ПРОТИВОСТОЯНИИ ИМ. ***МЫ ГОРДИМСЯ ТЕМ, ЧТО НАМ УДАЛОСЬ ДОСТИЧЬ.***

~ ШТАБНОЙ ГЕНЕРАЛ-МАЙОР АБДУЛАЗИЗ САЛЕХ АЛЬ СУЛАИТИ

Афганские беженцы позируют фотографу на военно-воздушной базе Аль Удеид после того, как их удалось спасти совместными усилиями Катара и Соединенных Штатов. РЕЙТЕР

Катар принимает участие в эвакуации граждан Афганистана и других стран. УПРАВЛЕНИЕ МОРАЛЬНЫХ ОРИЕНТИРОВ

Катар предоставляет медицинскую помощь афганским беженцам. УПРАВЛЕНИЕ МОРАЛЬНЫХ ОРИЕНТИРОВ

как было согласовано. Эти самолеты продолжали перевозить беженцев из Кабула в Катар, и их число постоянно множилось. Мы достигли такого этапа, когда к середине дня к нам прибывало 900 беженцев каждые 90 минут. Число беженцев достигло 4 тыс. человек в день, и мы должны были предоставить средства передвижения. Аэропорт не мог принимать более 10 тыс. беженцев за 5-6 часов, и транспортировка такого огромного количества людей представляла собой значительную трудность. Все взлетно-посадочные полосы были заняты, иногда на них, помимо самолетов из других стран, находилось 40 самолетов С-17. Все это требовало отлаженного командного подхода и высокого уровня координации действий.

Мне повезло в том, что я работал бок о бок с командующим военно-воздушными силами Центрального командования США генерал-полковником Грегори Гиллотом и командующим 379-й экспедиционной эскадрильей генерал-майором Джеральдом Донахью. Наша встреча произошла в аэропорту, где мы совместно преодолевали трудности и препятствия.

Расквартированные на базе Аль Удеид американские военнослужащие также не жалели усилий. На каждые 3 тыс. беженцев был выделен полковник сухопутных сил США со всеми его офицерами, которые работали круглосуточно без перерывов бок о бок с военнослужащими Катара и сотрудниками Министерства иностранных дел. Наши совместные действия увенчались успехом. Я помню день, когда посол Хольтц сказала, что все иностранные рейсы будут приостановлены, и будут приниматься только рейсы из Кабула. Она предупредила, что через несколько часов количество прибывших афганцев увеличится во много раз, и что уже сделанных приготовлений будет недостаточно. Она признала, что мы столкнемся с многочисленными трудностями, и что перед нами встанет выбор – принимать рейсы из Кабула или наложить запрет. Это решение должно было принять высшее командование, поэтому мы проинформировали об этом начальника штаба. Он связался с министром обороны, а затем с верховным главнокомандующим страны, и они решили, что мы будем продолжать принимать беженцев и оказывать поддержку нашему стратегическому союзнику, Соединенным Штатам, в принятии беженцев и предоставлении им убежища.

После получения одобрения ожидалось, что прибудет еще 30 тыс. человек; в страну уже прибыло 16 тыс. беженцев, так что общее число должно было быть 46 тыс. человек. Такое огромное количество было за гранью возможностей наших лагерей, и поэтому я связался с начальником Отдела США в Министерстве иностранных дел послом Иссой Аль-Маннаи. Мы приняли решение выделить самолет для транспортировки беженцев.

Я попросил посла Иссу направить запрос в Министерство иностранных дел. Я также детально описал ситуацию начальнику штаба генерал-полковнику Ганему бин Шахину Аль-Ганему, особо подчеркнув, через что пришлось пройти беженцам за последние 5-7 дней. Они были без крыши над головой и продовольствия до того, как прибыли в нашу страну, а экстремальная жара еще больше истощила их силы. Я направил запрос выделить самолет С-17, хотя у нас их ограниченное количество, и некоторые находились на выполнении других заданий. Начальник штаба направил запрос министру по делам обороны д-ру Халиду бин Мухаммеду Аль-Атийя, который затем представил этот запрос Его Высочеству эмиру. Эмир своим решением выделил 10 катарских самолетов для транспортировки беженцев, что было огромным шагом в уменьшении такого большого скопления людей. После того, как первые десять самолетов занялись транспортировкой беженцев, мы запросили еще 10 самолетов для этих же целей и получили их. Кроме того, для размещения личного состава и его оборудования был выделен госпиталь Аль-Вакра, что стоило Вооруженным силам Катара более 35 млн. долл. США.

Во время кризисных ситуаций, особенно во время гуманитарных кризисов, роль союзников заключается в совместном противостоянии им. Мы гордимся тем, что нам удалось достичь. Мы являемся союзниками Соединенных Штатов уже много лет. В 1990-х гг. подразделения США сосредоточились на границе Катара, и они были размещены в полевых лагерях, которые со

Власти Катара предоставили передвижные душевые и умывальники для эвакуированных афганцев на время их промежуточной чрезвычайной остановки на базе Аль Удеид. РЕЙТЕР

временем превратились в военно-воздушную базу Аль Удеид. Это было и остается частью нашей подготовки к поддержке нашего союзника, Соединенных Штатов. И наиболее ярким тому примером является база Аль Удеид. Это совместная база, на которой расположены войска Катара и США. В последние годы Вооруженные силы Катара все больше используют американские вооружения. Партнерство между нашими двумя странами повысило уровень подготовки наших сил, а также присутствие американских войск на нашей базе способствует стабильности в регионе. Мы благодарны американским военным за те усилия, которые они для этого прилагают. Строительство военно-воздушной базы Аль Удеид находится на начальной стадии, и у нас есть планы поэтапного комплексного развития этого района для большего удобства размещения военных Катара и США (проект «Развитие военно-воздушной базы Аль Удеид»).

«Unipath»: Что бы Вы хотели сказать в заключение?

Генерал-майор Аль-Сулаити: Я хотел бы отдать должное командному духу и позитивной атмосфере, царившим в ходе проведения операции по эвакуации беженцев. Я должен поблагодарить всех, кто оказал помощь в выполнении этой сложной гуманитарной миссии. Этих результатов невозможно было бы достичь без поддержки Его Высочества эмира Катара шейха Тамима бин Хамада Аль Тани, а также последующих действий со стороны заместителя премьер-министра и министра обороны Его Превосходительства д-ра Халеда Бин Мухаммеда Аль-Аттийя. Эта операция проводилась также под непосредственным контролем во стороны генерал-полковника Ганема бин Шахина Аль-Ганема, бывшего в то время начальником штаба, при поддержке и непосредственном участии ВВС эмира под командованием генерал-полковника Салема бин Хамада Аль-Набита, в настоящее время занимающего должность начальника штаба Вооруженных сил Катара. Я бы хотел также выразить благодарность и основным силам, а именно сотрудникам Военной полиции, Логистической службы, Оперативного управления и командованию базы Аль Удеид. Особая благодарность командующему базой генерал-майору Юссефу Шахину Аль-Атику, а также Управлению разведки и Управлению международного военного сотрудничества.

Что касается невоенных организаций, то следует помнить об особо важной роли, которую сыграло Министерство иностранных дел. В этой связи я хотел бы выразить особую признательность заместителю министра иностранных дел Его превосходительству Лулуа Аль-Хатеру, директору Отдела США в МИД Исса Мухаммеду Аль-Маннаи и всем задействованным сотрудниками МИД Катара. Отдельно хочу поблагодарить Министерство внутренних дел, особенно Его Превосходительство генерал-лейтенанта Абдуллу Аль-Мала и всех его сотрудников. Благодарю также Таможенную службу, Министерство здравоохранения, Министерство городского строительства и всех тех, кто внес свой вклад в успешное проведение этой гуманитарной миссии. Без божественного провидения и поддержки всех этих людей и организаций сложившаяся ситуация превратилась бы в гуманитарную катастрофу. Огромное всем спасибо! Да хранит Бог руководителей, народ и правительство Катара! ✦

ИЛЛЮСТРАЦИЯ «UNIPATH»

УКРЕПЛЯЯ ВОЕННЫЕ КОМПЬЮТЕРНЫЕ СЕТИ

Министерство обороны Ирака призывает на службу группу экспертов по вопросам кибербезопасности с целью обнаружения и предотвращения нападений

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Со стремительным развитием Интернета и мобильных телефонов технологический прогресс стал неотъемлемой частью повседневной жизни людей. Эти технологии усовершенствовали практически все сферы жизни общества, включая образование, медицину, инженерно-техническую деятельность, сферу безопасности и экономику. Однако, эти технологии поставили себе на службу также и организованные преступные группировки и террористы, что вынудило страны сформировать группы экспертов по кибербезопасности для защиты компьютерных сетей от кибернападений. Корреспондент журнала «Unipath» встретился со штабным генерал-лейтенантом Раадом Шакиром аль-Канани, начальником Управления военных коммуникаций Министерства обороны Ирака, для обсуждения задач и достижений министерской группы экспертов по кибербезопасности.

«Unipath»: *Какие шаги предприняло ваше управление, чтобы обезопасить Ирак от кибернападений?*

Генерал-лейтенант Раад: Основная задача Управления военных коммуникаций состоит в защите систем и сетей Министерства обороны Ирака, а также в разработке особых правил использования оборудования и сетей, принадлежащих министерству и его подразделениям. Для этого управление внедряет меры безопасности и руководящие указания, которые обеспечивают эффективность процедур по предотвращению кибератак.

Чтобы секретные конфиденциальные сети оставались закрытыми для общего доступа и не были связаны с общественными сетями, такими как Интернет, мы сотрудничаем с управлением создания и администрирования компьютерных сетей. Совместно с соответствующими техническими управлениями мы также разрабатываем и другие необходимые процедуры. Закрытая сеть – это сеть, содержащая электронную переписку военных, веб-сайты и контракты. У нас также есть другая онлайновая сеть для общественности, которая отделена от закрытой сети. Она управляется через официальный веб-сайт министерства и поддерживает связь с общественностью.

Мы также проводим занятия по информированию пользователей сетей об опасностях кибертерроризма и необходимости следовать правилам министерства для защиты сети от возможных взломов. Кроме того, мы особо подчеркиваем недопустимость использования в компьютерах министерства CD-ROM и персональных USB для просмотра фильмов или онлайновых игр, а также введён строгий запрет на загрузку внешних программ на аппаратуру министерства.

«Unipath»: *Как министерство сотрудничает с другими органами обеспечения безопасности в целях повышения уровня кибербезопасности?*

Генерал-лейтенант Раад: Мы поддерживаем прямое сотрудничество с другими органами, отвечающими за сферу кибербезопасности, посредством создания объединенных комитетов, таких как Верховный комитет коммуникаций и информационной безопасности и комитет, разрабатывающий национальную стратегию кибербезопасности. Также обсуждается сотрудничество с Национальной группой реагирования на компьютерные инциденты и выработка законодательства о наказании за киберпреступления. Сотрудничество в этой сфере чрезвычайно важно для обеспечения безопасности

национальных сетей и для установления хороших отношений со специалистами из других органов безопасности с тем, чтобы происходил обмен информацией и были выработаны оптимальные методы борьбы с угрозами и нападениями. Эти усилия являются дополнением к работе с нашими друзьями из сил коалиции через механизм Объединенного оперативного командования, где происходит обмен разведывательной информацией в сфере кибербезопасности и сбор разведданных с компьютеров из укрытий террористов и при помощи хакерских нападений на программы и вебсайты противника, что дает нам возможность противостоять террористическим нападениям на наши собственные сайты.

«Unipath»: *Какова ваша роль в защите центров голосования от нападений в режиме онлайн?*

Генерал-лейтенант Раад: Перед нами, как перед министерством обороны, поставлена задача защищать центры голосования от обычных террористических нападений и бунтов, и перед Управлением военных коммуникаций не стоит задача защиты их от кибератак. Тем не менее, как я уже отметил, мы сотрудничаем с другими органами, отвечающими за кибербезопасность, защищая национальную сеть от внешних нападений. Пока что к нам не поступала информация о подозрительной деятельности или попытках взлома сетей на избирательных участках.

«Unipath»: *Ваши обязанности ограничиваются только защитой объектов Министерства обороны, или в них включены и другие объекты государственного и частного секторов?*

Генерал-лейтенант Раад: В обязанности Управления военных коммуникаций входит только защита объектов Министерства обороны совместно с соответствующими техническими управлениями. Однако, невозможно провести четкую разграничительную линию между кибербезопасностью сетей нашего министерства и сетей других правительственных учреждений. Поэтому мы следим за тем, чтобы не было взломов сетей министерства, а также за тем, чтобы наши сети не стали ботами для нападения на другие чувствительные правительственные вебсайты. Для этого требуется обучение нашего персонала по таким вопросам как риск киберугроз и процедуры обеспечения безопасности сетей. Наряду с тем, что мы находимся в состоянии готовности защитить сеть от внешних угроз, мы еще отслеживаем входящую и выходящую онлайновую информацию сети министерства, а также выходящую информацию других правительственных учреждений. У нас есть постоянно обновляемые приложения, отвечающие за обнаружение вредоносных программ и защиту от вирусов.

«Unipath»: *Как вы предотвращаете использование незащищенной аппаратуры?*

Генерал-лейтенант Раад: Чтобы идти в ногу со стремительным глобальным технологическим развитием, в Министерстве обороны недавно было создано Управление кибербезопасности. Поскольку до 2003 г. Ирак был изолирован от всего остального мира, за последние два десятилетия мы не могли угнаться за технологическим прогрессом. Среди военных предпочитаемой формой коммуникаций стали мобильные телефоны. Было просто невозможно объяснить всем воинским подразделениям недопустимость использования мобильных телефонов при военных коммуникациях или для передачи с поля боя информации о военных операциях. Мы наблюдали случаи нарушения правил военнослужащими, делавшими телефонами фотографии или видеосъемку поля боя, а также использование мобильных телефонов командующими формированиями во время боя. В этой связи были предприняты необходимые меры. Для предотвращения использования незащищенной и незашифрованной аппаратуры и средств коммуникаций существуют специальные инструкции и руководящие указания. Разрешается пользоваться исключительно защищенными и зашифрованными устройствами, одобренными Управлением военных коммуникаций. Однако, подобные нарушения имеют место даже в самых передовых армиях. Поэтому всем формированиям должны быть приданы офицеры, отвечающие за информационную безопасность, которые должны быть обучены группой специалистов по кибербезопасности. Эти офицеры, в свою очередь, должны довести существующие правила до рядовых военнослужащих.

«Unipath»: *В сентябре 2021 г. Вы принимали участие в работе конференции на тему «Группа реагирования на инциденты в сфере кибербезопасности». Вы можете рассказать о рекомендациях, высказанных на этой конференции?*

Генерал-лейтенант Раад: Материалы конференции имеют чрезвычайную важность, поскольку обсуждаемые на ней темы имели непосредственное отношение к нынешним реальным угрозам. Я рад, что смог принять участие в работе конференции и познакомиться с нашими братьями из служб безопасности, узнать об их опыте работы в реальных условиях и увидеть применение новейших тактических приемов. Что касается рекомендаций, высказанных на этой конференции по вопросам кибербезопасности, то они были следующие:

1. Выступить с инициативой создания программы по усилению кибербезопасности для всех государственных учреждений.
2. В рамках министерства высшего образования

и научных исследований разработать академический учебный план и специализированные программы аспирантуры по вопросам кибербезопасности.

3. Привлечь компетентных специалистов посредством создания ассоциации экспертов, любителей и профессионалов в сфере кибербезопасности. Для реализации этой идеи, при поддержке общественных организаций и частного сектора был создан Фонд развития общественной инициативы.
4. Иракская Группа реагирования на чрезвычайные компьютерные ситуации, Министерство высшего образования и научных исследований, частные компании и международные организации согласились создать свои местные группы реагирования. Иракская группа реагирования на чрезвычайные компьютерные ситуации приняла свод правил для компаний, работающих в сфере кибербезопасности, а также стратегический план повышения позиции Ирака в Глобальном индексе кибербезопасности.

«Unipath»: *Как министерство отбирает и готовит группу специалистов по кибербезопасности?*

Генерал-лейтенант Раад: Члены группы отбираются из персонала специализированного технического отдела Министерства обороны Ирака. Члены группы – офицеры и инженеры – должны быть опытными, квалифицированными специалистами в области кибербезопасности, и кандидаты должны пройти проверку и получить одобрение служб безопасности.

«Unipath»: *Насколько строги законы, в соответствии с которыми в Ираке судят киберпреступников?*

Генерал-лейтенант Раад: По состоянию на конец 2021 г., в Ираке еще не принят закон о наказании за киберпреступления, но его проект ожидает одобрения Совета представителей, после чего он должен быть ратифицирован правительством. Мы с нетерпением ждем принятия этого закона, который будет наказывать и сдерживать киберпреступников и предотвратит использование организованными киберпреступными группировками национальной сети Ирака в качестве пусковой площадки для нападений на другие государственные системы с целью вымогательства или диверсий.

«Unipath»: *Каков уровень вашего сотрудничества с дружественными странами в вопросе совершенствования кибертехнологий?*

Генерал-лейтенант Раад: Ответственность за кибербезопасность распространяется на всех, и даже отдельные случаи взлома сетей могут напрямую затронуть все страны мира. Когда я говорю «отдельные случаи», то имею ввиду случаи, имеющие место в местах, изолированных в географическом смысле, а не случаи, изолированные в смысле охвата электронными средствами коммуникации. В наш цифровой век весь мир взаимосвязан, в нем нет полностью изолированных мест. Наравне с огромными преимуществами эта взаимосвязанность принесла нам и большие риски, и поэтому мы проявляем бдительность и сдерживаем всех, кто склонен использовать информационные технологии в преступных целях либо на местном уровне, либо транснационально. Интернет, электронная почта и страницы в социальных сетевых ресурсах сузили огромный мир до размеров небольшой деревни, в которой вредоносные программы и вирусы распространяются гораздо быстрее. Именно поэтому чрезвычайно необходимо международное сотрудничество и обмен информацией между союзными странами. Сотрудничество с союзными странами может принимать формы специальных курсов по вопросам кибербезопасности или проведения соревнований «Кибервоинов», организованных в 2020 г. Отделом оборонного сотрудничества посольства США. Такие курсы и соревнования приносят большую пользу их участникам.

«Unipath»: *Каким образом Управлению связи и коммуникаций Министерства обороны удается идти в ногу с быстрым развитием технологий?*

Генерал-лейтенант Раад: У нас есть группа, которая специализируется на исследованиях и отслеживании технологического развития; мы также стремимся участвовать в конференциях и семинарах по вопросам кибербезопасности. Мы сотрудничаем с министерскими научно-исследовательскими центрами и техническими университетами с целью повышения профессионального уровня наших сотрудников. Кроме того, мы планируем послать наших сотрудников на специализированные курсы в страны НАТО или союзные страны. Мы стремимся привлечь людей с выдающимися способностями из среды выпускников иракских университетов и сотрудников Министерства обороны с тем, чтобы сохранить высокий уровень эффективности нашей работы.

«Unipath»: *Осуществляла ли Даиш кибернападения на веб-сайты Министерства обороны?*

Генерал-лейтенант Раад: Нет, Даиш раньше не нападала на вебсайты Министерства обороны. Причиной тому, возможно, был высокий уровень технической защиты сети министерства и опыт команды сотрудников сферы информационной безопасности, а также тот факт, что наша сеть, регистрирующая передвижение вооружений и войск, является закрытой. ✦

СОХРАНЕНИЕ ТЕРРИТОРИАЛЬНОЙ ЦЕЛОСТНОСТИ ЙЕМЕНА

ВМЕШАТЕЛЬСТВО ИРАНА МЕШАЕТ ЙЕМЕНЦАМ ВЕСТИ ПЕРЕГОВОРЫ О ПОЛИТИЧЕСКОМ УРЕГУЛИРОВАНИИ ГРАЖДАНСКОЙ ВОЙНЫ В СТРАНЕ

Д-Р АХМАД АВАД БЕН МУБАРАК, МИНИСТР ИНОСТРАННЫХ ДЕЛ ЙЕМЕНА

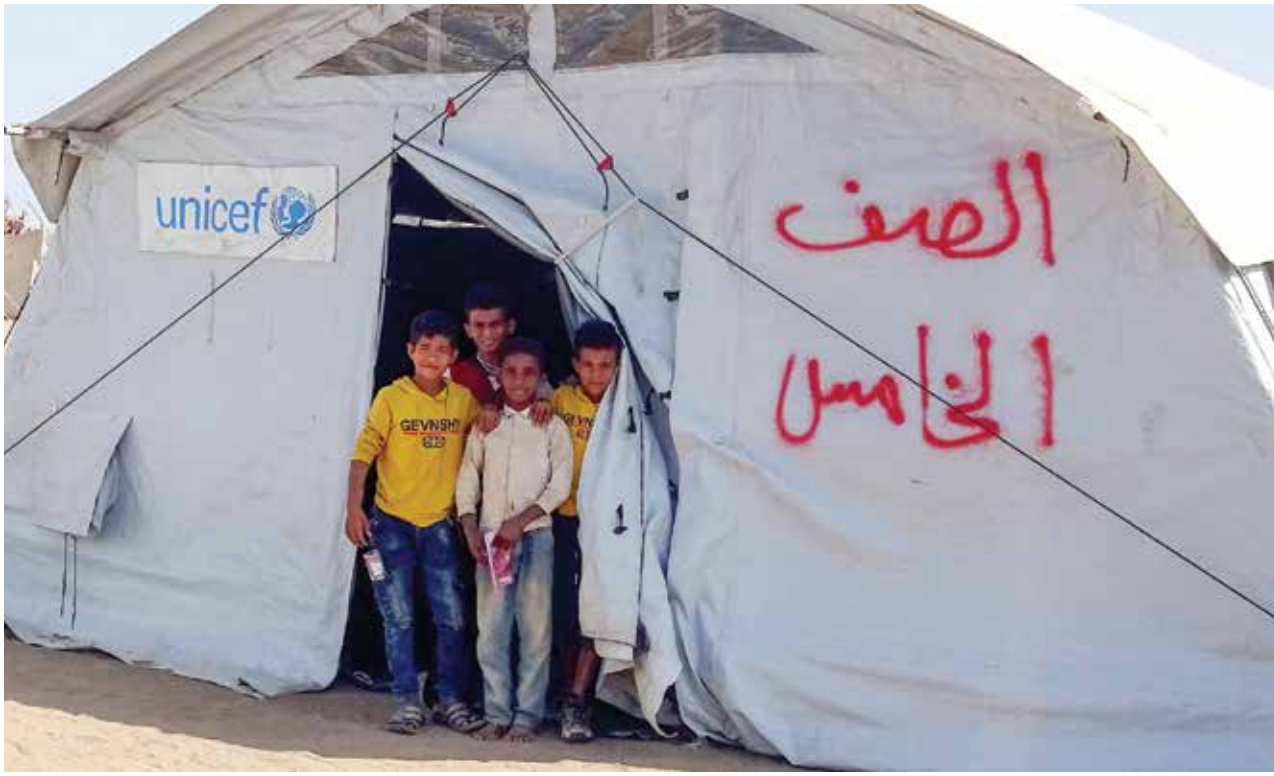
Война в Йемене длится уже седьмой год, начавшись с тех пор, как повстанцы-хуситы развязали ее против йеменского народа после государственного переворота, совершенного против законной власти. Эта война опасна не только потому, что повстанцы-хуситы пытаются захватить власть, но и потому, что они также стремятся изменить характер йеменского общества, подорвать его будущее и будущее региона, массово вербуя детей и настраивая молодежь на насилие, разжигание конфликтов и распространение ненависти между жителями одной и той же страны. Кроме того, хуситы пытаются распространить в обществе невежество, чтобы облегчить контроль над ним; они стремятся ввергнуть йеменцев в нищету и использовать их для участия в войнах. Все это создало благоприятную среду для превращения Йемена в один из столпов экспансионистской стратегии Ирана в регионе.

План Ирана теперь ясен. Его незаконные формирования окружают Аравийский полуостров. После того, как Иран приобрел высококачественный военный потенциал, опасность возросла. Нет никаких сомнений в том, что провал иранского проекта в Йемене приведет к провалу иранского проекта во всем регионе. Его успех в Йемене откроет новую фазу конфликта и приведет к новому циклу насилия и хаоса. Я попытаюсь прояснить, где мы находимся сегодня, и какова наша стратегия достижения мира в Йемене.

В центре внимания тех, кто следит за йеменскими событиями, на данном этапе войны находится мухафаза Мариб. С ноября 2020 г. хуситы начали непрерывное наступление на Мариб. Это нападение продиктовано злобой, которая не менее пагубна, чем иллюзия того, что повстанцы могут захватить эту мухафазу, и еще большая иллюзия того, что Йемен можно контролировать с помощью насилия, терроризма и военной силы.

Мухафаза Мариб, наряду с историческим значением, приобрела национальное и стратегическое значение. Многие, возможно, забыли, что эта мухафаза в 2015 г. разгромила хуситов, имея скромные боевые возможности по сравнению с тем, что она имеет сегодня, обладая населением не более 350 тыс. человек. Сегодня её возможности возросли. Имея население в 4 млн. человек, из которых 2 млн. являются внутренне перемещенными лицами, она стала убежищем

Солдат, верный законному правительству Йемена, осматривает линию фронта в мухафазе Мариб, где хуситы продолжают боевые действия, несмотря на международные попытки добиться прекращения огня. AFP/GETTY IMAGES



Йеменские дети ходят в школу в лагере для перемещенных лиц в Ходейде – это жертвы войны, окончание которой хуситы затягивают в угоду Ирану. Из-за войны 2 млн. школьников не имеют доступа к систематическому школьному образованию.
AFP/GETTY IMAGES

для йеменцев различных социальных и политических убеждений. Её население поддерживает армию, верящую в народ и имеющую твердую и несокрушимую волю положить конец планам хуситов.

Несмотря на это, необходимо отметить, что некоторые причастные стороны просчитались, начав говорить о сценарии, который последует после Мариба. Если обсуждать сценарий, который для нас нереалистичен, мы, несомненно, скажем, что, если хуситы получат контроль над Марибом, это будет так же плохо, как если бы была разрушена его знаменитая с давних времен плотина. Мариб для Йемена сегодня — это неприступная стена. Он стал одним из стратегических приоритетов иранского режима. Падение Мариба не только привело бы к ужасающей гуманитарной ситуации, но и ознаменовало бы конец процесса политического регулирования и установления мира в Йемене. Оно положило бы конец усилиям по восстановлению безопасности и стабильности. Воцарился бы хаос; последовало бы еще больше насилия, внутренних раздоров и волн миграции. Это стало бы началом длительного состояния нестабильности, которое может привести к другим войнам, ведущимся из Йемена по отношению к остальной части региона.

Наша стратегия и подход правительства Йемена таковы: альтернативы миру в Йемене нет. Любой справедливый, всеобъемлющий и устойчивый мир должен быть направлен на устранение политических причин войны, заключающихся в попытках хуситов силой навязать Йемену свой контроль и гегемонию.

Несмотря на разрушительную интервенцию Ирана в Йемене, несмотря на его военную поддержку ополчения хуситов и финансирование его военной машины, отношение к войне в Йемене как к региональной войне чужими руками является заблуждением, и его следует исправить. Никакое мирное урегулирование в Йемене не может быть успешным, если йеменцы не согласятся решать свои внутренние проблемы в соответствии с итогами Конференции по всеобъемлющему национальному диалогу и принципам справедливого распределения власти и богатства.

Однако, в то же время было бы неправильно пренебрегать геостратегическим аспектом иранского вмешательства в Йемен и стремлением Ирана стать ближе к Красному и Аравийскому морям. Такой ход событий повысит стратегическую заинтересованность Ирана в конфликте и усилит региональную и международную конкуренцию.

Иранские инвестиции в движение хуситов начались давно и увеличились в начале второго тысячелетия. Захват ВМС США за несколько лет до войны иранских кораблей «Джихан-1» и «Джихан-2», направлявшихся к хуситам с оружием и ракетами, доказывает это. Это позволяет нам, по сути, развенчать утверждение о том, что причиной иранского вмешательства в Йемен является нынешняя война.

Среди заблуждений мы также можем упомянуть утверждение, что хуситы отвергают мир всякий раз, когда они делают успехи в военном отношении. В действительности, они отвергают мир как стратегический принцип, независимо от того, наступают они или отступают в военном отношении, рассматривая мир как тактику в рамках своей военной стратегии. У нас есть десятки свидетельств этого. Наиболее очевидным свидетельством, вероятно, является Стокгольмское соглашение, которое ополчение

Военный корабль США захватывает судно, перевозившее химические удобрения в Йемен для изготовления взрывчатки. АССОШИЭЙТЕД ПРЕСС

хуситов приняло в декабре 2018 г. и так и не выполнило ни одного из его положений.

Понимание этого факта помогает нам осмыслить правильный подход к достижению мира с группировкой, которая основывает свои расчеты не на фактах, а скорее на теократическом мышлении, базирующемся на иллюзии божественного права на правление. Это самое серьезное препятствие, которое сорвало достижение соглашения во всех раундах мирных переговоров, от Женевы до Кувейта, и даже в Стокгольмском раунде. Если мы примем во внимание этот очевидный факт, мы можем сказать, что самым важным тестом намерений ополчения хуситов — тестом, который оно постоянно проваливает — является принятие соглашения о всеобъемлющем прекращении огня в качестве важнейшего гуманитарного шага. Все другие гуманитарные вопросы могут быть решены до начала переговоров по поиску всеобъемлющего политического решения.

Мы считаем, что сплоченность и единство всех умеренных политических сил, выступающих против иранских планов в Йемене, является первым необходимым условием для политического урегулирования. Эр-риядское соглашение могло бы быть заключено и реализовано в дополнение к приложению по вопросам безопасности и военным вопросам, поскольку они представляют собой важнейшую основу для достижения мира, безопасности и стабильности.

Региональная и международная поддержка йеменского правительства в преодолении его экономических проблем и укреплении политического, экономического и гуманитарного партнерства позволит правительству сохранить умеренный Йемен, разделяющий с остальным миром общие гуманитарные ценности и принципы. Мы понимаем важность продолжения усилий стран региона и всего мира по оказанию давления на Иран с целью прекращения его подрывной деятельности в Йемене, после чего на Ближнем Востоке воцарятся безопасность, мир и стабильность.

Для того, чтобы обуздать повстанцев и решить вопросы и проблемы, которые они вызвали в йеменском обществе, достаточно достижения мира в нашей стране. Вот почему для достижения всеобъемлющего, справедливого и прочного мира, для восстановления безопасности и стабильности в Йемене нам необходимо подходить гибко ко всем усилиям, направленным на достижение мира в соответствии с нашими национальными принципами, Инициативой Совета сотрудничества арабских государств Арабского залива и механизмом её реализации, итогами Конференции по всеобъемлющему национальному диалогу и Резолюцией 2216 Совета Безопасности Организации Объединенных Наций.

В заключение я упомяну о катастрофической экологической опасности, которую все ожидают, фактически не прилагая никаких реальных усилий, чтобы избежать ее – утечка более 1 млн. баррелей сырой нефти, хранящейся в течение семи лет в нефтяном танкере «Сафер», будет настоящей катастрофой, которая разрушит морскую среду Йемена и региона, особенно Красное море и прилегающие к нему районы. Хуситы все еще удерживают танкер в заложниках. Они отказываются дать разрешение группе Организации Объединенных Наций на его техническое обслуживание. ✦

Это слегка сокращенная версия речи, произнесенной на 17-м саммите по региональной безопасности в Бахрейне в ноябре 2021 г. в рамках Манамского диалога.

ЗАЩИЩАЯ цифровую собственность Пакистана

ИЛЛЮСТРАЦИЯ «UNIPATH»

СТРАНА ПРИНИМАЕТ СВОЮ ПЕРВУЮ НАЦИОНАЛЬНУЮ ПОЛИТИКУ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ С ЦЕЛЬЮ ОГРАДИТЬ СВОИ СЕТИ ОТ НАПАДЕНИЯ

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Озабоченное возможными кибератаками на компьютерные сети, федеральное правительство Пакистана в июле 2021 г. одобрило первую в стране Национальную политику в сфере кибербезопасности. Министерство информационных технологий и коммуникаций Пакистана разработало эту политику для того, чтобы защитить цифровые активы государства от киберпреступников и потенциальных геополитических противников.

Политика Пакистана разбита на ряд пересекающихся категорий – юридическую, техническую и организационную, чтобы улучшить защиту подсоединенных к Интернету устройств, уровень защиты которых министр информации страны счел недостаточным. Более 65 млн. пакистанцев имеют Интернет, и страна, как и многие другие страны в мире, переводит бизнес и правительственные услуги в режим онлайн.

Пакистан будет реализовывать принятую политику в рамках уже существующих правительственных групп реагирования на чрезвычайные компьютерные ситуации.

«Министерству информационных технологий и всем соответствующим общественным и частным организациям будет предоставлена вся возможная помощь и поддержка, чтобы гарантировать соответствие их информации, служб, информационных и коммуникационных технологий требованиям кибербезопасности», - объявил министр информационных технологий и коммуникаций Пакистана Сайед Аминул Хак.

Вот примеры указаний, содержащихся в новой политике кибербезопасности Пакистана:

- Создание Комитета по политике киберуправления для надзора за стратегией кибербезопасности страны.
- Осуществление «активной обороны» для предотвращения фишинга электронной почты, проникновения в правительственные сети и заражения вирусами.
- Защита и повышение жизнестойкости национальной критически важной информационной инфраструктуры и правительственных информационных систем.
- Стимулирование партнерства между общественным и частным секторами для использования предпринимательских новшеств, выгодных для Пакистана.
- Проведение и спонсирование научно-исследовательских разработок в сфере кибербезопасности, включая повышение качества обучения персонала.
- Содействие выработке национальной культуры кибербезопасности, при которой пользователи компьютеров и смартфонов обучаются методам защиты важной информации.
- Повышение уровня глобального сотрудничества и взаимодействия, направленного на повышение рейтинга Пакистана в международных индексах кибербезопасности.
- Создание механизма реагирования на киберпреступления, включая усовершенствование законодательной и регуляторной базы.
- Установление доверия к цифровым транзакциям путем использования улучшенных механизмов сертификации и верификации.
- Пакистанский журналист Джехангир Мудассар, специализирующийся на вопросах технологий и пишущий для пакистанского военного журнала «Hilal», подчеркнул, что защита компьютеров и сотовых телефонов от нападений требует определенных сдвигов в информированности всего общества.

«Кибербезопасность заключается не в том, чтобы нажатием кнопки активировать определенный протокол. Это культура, которая должна стать частью образа жизни всех наших людей – простых граждан, государственных служащих и сотрудников сил безопасности, - пишет Мудассар. – Для повышения уровня нашей кибербезопасности в настоящее время и в будущем, частью наших правил поведения должна стать комплексная политика в этой сфере, соблюдаемая всеми заинтересованными сторонами». ✦

Источники: Министерство информационных технологий и телекоммуникаций Пакистана; «Hilal»; «Dawn»; «Eurasia Review»

Пакистанские торговцы загружают файлы с компьютеров в мобильные телефоны в г. Файсалабад. Рост числа пользователей информационных технологий в стране требует от правительства более жестких правил кибербезопасности. AFP/GETTY IMAGES

ИЛЛЮСТРАЦИЯ «UNIPATH»

НЕОБХОДИМОСТЬ УЛУЧШИТЬ РАБОТУ РАЗВЕДКИ

ИССАМ АББАС АМИН, УПРАВЛЕНИЕ РАЗВЕДКИ И БЕЗОПАСНОСТИ, МИНИСТЕРСТВО ОБОРОНЫ ИРАКА

Разведсообщество испытывает давление из-за нереалистичных ожиданий относительно возможностей предотвращения непредвиденных событий, особенно тех, которые направлены на подрыв государственного суверенитета или внутренней безопасности. Примером могут служить два нападения с использованием дронов на дом премьер-министра Ирака 7 ноября 2021 г.

По самой своей природе неудачи разведки всегда поднимают вопрос о компетентности разведслужб и методах их работы по предотвращению брешей в системе безопасности.

Проблема разведки состоит в том, что ее постоянно можно подвергать критике. Даже хорошо себя зарекомендовавшие разведслужбы, например, разведслужбы США, в своей деятельности допускали стратегические просчеты. На память приходят такие примеры как нападение на Перл Харбор в 1941 г., вторжение Северной Кореи в Южную Корею в 1950 г., советская интервенция в Чехословакию в 1968 г. и нападения 11 сентября 2001 г. Иногда разведке не удается заранее предупредить о готовящемся событии, как это было в случае нападений 11 сентября 2001 г., или она давала множество неверных предупреждений, как это было в вопросе об обладании Ираком оружием массового уничтожения.

В обоих случаях промахи разведки были очевидны, а критика уничтожающей. Превалирующее в этом вопросе мнение состоит в том, что разведка всегда и во всем должна делать правильные выводы. В реальном мире этого достичь невозможно, и это становится источником сильного раздражения и разочарования, когда случается что-то непредвиденное.

Разведорганы могут играть свою роль относительно неплохо, если вопрос связан с политикой соседнего государства, такого как Иран, или с тем, какой будет нанесен ущерб Ираку, если он подвергнется нападению в конкретном районе. Такой тип разведывательной информации представляет собой ответ на вопросы, имеющие разные варианты ответов, и способность понять тематику зависит больше от правильности предположений, чем от достоверности информации.

Но что, если вопрос стоит, например, так: когда и где Даиш совершит следующее нападение? Это уже другое дело, потому что точный ответ требует проникновения в самое сердце организации, что зависит от наших возможностей сделать серьезный прорыв в методах сбора информации.

Кроме того, повысить качество разведывательной работы трудно, особенно в том, что касается аналитических методов в вопросе предотвращения непредсказуемых событий. Несмотря на улучшение методов и средств сбора информации, степень достоверности разведывательного анализа и разведывательной оценки обстановки остается на прежнем уровне. Неуверенность и сомнения все равно остаются, даже в тех случаях, когда имеется максимально достоверная и надежная информация.

Из этого можно сделать важный вывод о том, что разведорганы не в состоянии устранить элемент неожиданности. Разведслужбы хорошо справляются с задачей информирования принимающих решения руководителей об имеющихся

фактах, давая им возможность принимать решение на основе разумной уверенности в правильности этого решения. Это немаловажно и наблюдается не так часто.

На стратегическом уровне разведслужбы несут ответственность за разведывательную оценку обстановки в национальном масштабе, и эта оценка формирует политику и стратегию национальной безопасности, бюджет служб безопасности и состав вооруженных сил. Объединенный комитет начальников штабов Ирака в своем планировании опирается на такую оценку.

Также необходимо подчеркнуть различие между разведывательной оценкой обстановки на национальном уровне в отношении внешних угроз и угроз внутри страны. Ирак сейчас больше сосредоточен на внутренних угрозах, чем на внешних, и это – упущение, которое должно быть устранено.

Еще одно слабое место состоит в том, что сегодня аналитики в разведорганах привязаны к командной вертикали прямо до самого верха пирамиды. Это неизбежно оказывает влияние на их объективность и беспристрастность. Было бы предпочтительнее, чтобы при подготовке своих оценок для принимающих стратегические решения руководителей разведывательные отделы сохраняли определенную независимость.

Разведывательная оценка обстановки на национальном уровне чрезвычайно важна для направления действий политических лидеров. Эта оценка должна быть профессиональной, рациональной и пригодной для использования. Например, стратегическое предупреждение о войне, являющееся военно-политическим вопросом, может совместно оцениваться Генеральным управлением разведки и безопасности и Министерством иностранных дел, каждым ведомством в пределах своей компетенции.

РАЗВЕДЫВАТЕЛЬНАЯ ОЦЕНКА ОБСТАНОВКИ НА НАЦИОНАЛЬНОМ УРОВНЕ ЧРЕЗВЫЧАЙНО ВАЖНА ДЛЯ НАПРАВЛЕНИЯ ДЕЙСТВИЙ ПОЛИТИЧЕСКИХ ЛИДЕРОВ.

Четыре примера просчетов разведки, изменивших мир: (сверху вниз по часовой стрелке) вторжение Северной Кореи в Южную Корею в 1950 г., нападение на Перл Харбор в 1941 г., советское вторжение в Чехословакию в 1968 г. и нападение на США 11 сентября 2001 г.
AFP/GETTY IMAGES

Однако, эти два государственных органа не имеют достаточной степени интеграции, чтобы совместно составлять реалистичные предупреждения. Для этого необходим высокий уровень сотрудничества и координации действий и общий бюрократический язык составления документов.

Ввиду появления новых игроков, неспокойных арен конкуренции и динамичности развития событий, результаты которых трудно предсказать, разведывательная оценка обстановки превратилась в сложную и запутанную задачу. Кроме того, сложность возникает и из-за текущих социальных и культурных процессов, включая внедрение новых технологий, таких как социальные сетевые ресурсы, с которыми разведсообщество раньше не сталкивалось. Разведывательные отделы зачастую не имеют необходимых знаний, чтобы освоить эти новшества, что порождает многочисленные проблемы, вызовы и риски.

При нынешних условиях разведсообществу трудно предсказывать, что случится завтра, поскольку события развиваются очень быстро. Противники могут совершать действия в киберпространстве мгновенно, и для того, чтобы подготовить к запуску беспилотник или ракету, нужно совсем мало времени. Все это сокращает время, необходимое противнику на то, чтобы перейти от этапа обдумывания к этапу реализации. Именно это и произошло при нападении 7 ноября 2021 г. Оно застало врасплох не только премьер-министра, но и его разведслужбу. ✦

Разведывательная оценка обстановки состоит из следующих компонентов:

1. **Угрозы.** Здесь описываются возможности и намерения различных игроков и связи между ними, анализируются процессы и тенденции на организационном уровне и на уровне региональной и глобальной политики.
2. **Процессы**. Описывается вероятность длительных процессов и тенденций, представляются различные сценарии и анализируются потенциальные реакции игроков на конкретные события. Например, как отдельные игроки (внутри страны и за рубежом) ответят на определенные действия наших сил?
3. **Рекомендации.** Предоставляет советы по имеющимся рискам и возможностям.

С чувством глубокого сожаления мы сообщаем о кончине автора – Иссама Аббаса Амина. Его кончина стала большой утратой для читателей журнала «Unipath» и для Управления разведки и безопасности Министерства обороны Ирака.

ВМС

В СОСТОЯНИИ ГОТОВНОСТИ

ВООРУЖЕННЫЕ СИЛЫ ИОРДАНИИ

Интервью с командующим Королевским ВМС Иордании капитан 1 ранга Хишамом Халилом Аль-Джарра

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

«UNIPATH»: *Опишите обязанности Королевского ВМФ Иордании*

Полковник Аль-Джарра: Королевский военно-морской флот является одним из трех видов войск Вооруженных сил Иордани (сухопутные, воздушные и морские силы) и вносит свой вклад в национальную систему обороны, играя двойную роль – военную роль ВМФ и роль службы береговой охраны, отвечая за организационные вопросы и вопросы обеспечения безопасности. ВМФ считается основной морской силой, и в основном несет ответственность за обеспечение морской безопасности Иордании. Эта миссия предполагает выполнение ряда обязанностей, в числе которых патрулирование для защиты и охраны морских границ Иордании и предотвращение незаконного проникновения и контрабандных операций, военно-морская инспекция, проводимая квалифицированными и обученными группами инспекторов с использованием самого передового оборудования, обнаружение и предотвращение любых нарушений в региональных водах, применение принятых законов, а также надзор за гражданскими и военными объектами и критически важными целями в Акабе, осуществляемый через Центр военно-морских операций. Кроме того, мы занимаемся поисково-спасательными операциями в региональных водах и боремся с загрязнением морских вод.

«UNIPATH»: *С какими проблемами морской безопасности сталкивается ВМФ Иордании в Красном море?*

Полковник Аль-Джарра: Проблемы, с которыми сталкивается иорданский ВМФ в Красном море при выполнении своих обязанностей по обеспечению морской безопасности, принимают различные формы. Сюда входят неконвенциональные проблемы, такие как терроризм, проявляющийся в нападениях на суда и портовые сооружения, морское пиратство, угрожающее безопасности судоходства, а в последнее время и кризисная ситуация с распространением коронавируса, повлиявшая на морские транспортные перевозки. Некоторые из проблем имеют и конвенциональный аспект безопасности, например, незаконное проникновение и пересечение морских границ страны и любые формы контрабандных операций, а также и проблемы из разряда особых, например, инциденты и катастрофы на море, пожары на кораблях и в порту, загрязнение морских вод и забастовки рабочих. Учитывая весь набор этих проблем, необходимо, чтобы все ведомства, имеющие отношение к обеспечению морской безопасности, повысили уровень своего сотрудничества, эффективности и готовности.

«UNIPATH»: *Какую помощь могут оказать страны-партнеры в развитии ВМФ Иордании? Какие необходимы суда и оборудование?*

Полковник Аль-Джарра: Несомненно, международные и региональные партнеры играют значительную роль в совершенствовании возможностей военно-морского флота Иордании в таких аспектах как обучение и передача опыта посредством организации совместных курсов и военных учений. Они также удовлетворяют потребности иорданского ВМФ, обеспечивая наличие судов, способных действовать за пределами региональных вод и оснащенных необходимым высокоточным оборудованием, повышающим возможности быстрого реагирования и сокращающим время реагирования при чрезвычайных ситуациях. Само собой разумеется, что такое сотрудничество расширило возможности нашего 77-го батальона

морской пехоты, что позволяет ему в полном объеме выполнять свои обязанности. Стоит отметить тесное сотрудничество между ВМФ Иордании и ВМФ США и Корпусом морской пехоты США в этой области.

«UNIPATH»: *Есть ли сотрудничество в сфере безопасности с государствами, граничащими с заливом Акаба?*

Полковник Аль-Джарра: Конечно же, обязанность по обеспечению морской безопасности Иордании требует высокой степени сотрудничества и координации действий с государствами, имеющими выход к заливу Акаба. Это единственный морской порт Иордании, через который осуществляются международные перевозки. Естественно, осуществляется постоянное сотрудничество с прибрежными государствами через офицеров по связи и взаимодействию и посредством проведения периодических совещаний по вопросам безопасности. Такая координация действий и сотрудничество находят свое отражение в военно-морских учениях, проводимых этими странами.

«UNIPATH»: *Насколько важны совместные региональные и международные морские учения?*

Полковник Аль-Джарра: Проведение двусторонних или многосторонних военно-морских учений играет важную роль в достижении требуемого уровня сотрудничества и координации между флотами разных стран. Учения повышают эффективность и компетентность участвующих в них сил. Кроме того, все участвующие стороны обмениваются навыками и опытом, что способствует достижению более высокой степени унификации концепций и процедур ВМФ разных стран как на региональном, так и на глобальном уровнях.

«UNIPATH»: *Находясь в составе Объединенных морских сил, какие выгоды получила Иордания от обмена опытом с остальными 34 странами коалиции?*

Полковник Аль-Джарра: Королевский ВМФ Иордании был активным членом Объединенных морских сил с момента их создания в 2009 г. Участие в операциях Объединенных морских сил продемонстрировало эффективную роль и достойный подражания образ иорданских ВМФ, и, несомненно, членство в этой группе способствовало повышению квалификации иорданских военных моряков благодаря обмену опытом с участниками из стран коалиции, ознакомлению с особенностями работы международных военно-морских сил и изучению зарубежного опыта в проведении морских операций. В свою очередь, это положительно сказалось на стандартах уровня подготовки офицерского и сержантского состава, что впоследствии обеспечило более высокие стандарты

Иорданские морские пехотинцы проходят обучение и проводят операции в заливе Акаба. ВООРУЖЕННЫЕ СИЛЫ ИОРДАНИИ

ВООРУЖЕННЫЕ СИЛЫ ИОРДАНИИ

Полковник Хишам Халил Аль-Джарра, командующий Королевским ВМФ Иордании, справа, и командующий военно-морскими силами Центрального командования США вице-адмирал Брэд Купер осматривают новое автоматическое беспилотное судно Saildrone Explorer. Бахрейн, ноябрь 2021 г.

СТАРШИНА 2-ГО КЛАССА МАРК ТОМАС МАХМОД/ ВМФ США

обучения, квалификации и навыков всех моряков иорданского ВМФ. Кроме того, завязывались дружеские связи и проходили общественные и культурные обмены с участниками из других стран.

«UNIPATH»: *В каких учениях принимает участие Королевский ВМФ Иордании, и почему вы считаете это участие важным?*

Полковник Аль-Джарра: ВМФ Иордании принимает участие в различных учениях на трех уровнях: на местном и национальном, региональном и международном. На местном уровне ВМФ организует внутренние учения в рамках командования с целью повышения слаженности действий и сотрудничества между подразделениями. Некоторые учения проводятся на общенациональном уровне, и отдельные сценарии предполагают участие военных и служб безопасности, а также некоторых гражданских учреждений, находящихся в юрисдикции морских ведомств. Целью учений является достижение требуемого уровня сотрудничества и координации между отдельными боевыми группами и повышение возможностей реагирования на чрезвычайные ситуации. На региональном уровне ВМФ Иордании регулярно участвует в морских учениях совместно с государствами, имеющими выход к заливу Акаба. Учения проходят на территории Хашимитского королевства Иордании, это такие учения как «Стремительный лев» и «Вечный защитник», в Египте проходят учения «Яркая звезда», а Саудовская Аравия проводит учения «Красная волна» и «Безопасное

побережье». Что касается международного уровня, то военные моряки Иордании постоянно принимают участие в многочисленных военно-морских учениях в качестве активных участников или наблюдателей. Нет никаких сомнений в том, что такое постоянное присутствие на учениях позволяет иорданским военным морякам знакомиться с самыми последними методами оперативного управления и обмениваться опытом с другими участниками.

«UNIPATH»: *Как Корпус морской пехоты США помогает в развитии ваших военно-морских сил?*

Полковник Аль-Джарра: ВМФ Иордании через свой 77-й батальон морской пехоты поддерживает особые отношения с американскими морскими пехотинцами. Эти отношения проявились в совместной программе унификации, реализованной в течение нескольких лет и внесшей вклад в повышение боеготовности и уровня подготовки бойцов батальона для проведения оборонительных и наступательных операций, а также в подготовку подразделений спецназа и групп инспекторов кораблей. Следует отметить, что в рамках партнерства с американскими морскими пехотинцами 77-й батальон получил различное оборудование и сложные приборы, применяемые морскими пехотинцами в операциях. Важность этих отношений также проявляется в постоянном выполнении совместных задач и многоуровневой координации действий. Мы, как командование ВМФ Иордании, стремимся сохранять и развивать эти отношения в интересах обеих наших стран.

«UNIPATH»: *Как ВМФ Иордании взаимодействует с остальными службами безопасности в деле охраны территориальных вод страны?*

Полковник Аль-Джарра: За морскую безопасность Иордании совместно несут ответственность различные военные ведомства и службы безопасности, а также правительственные органы и учреждения, имеющие отношение к деятельности на море. Поэтому ВМФ Иордании осознает важность сотрудничества и координации усилий с различными ведомствами для достижения желаемого уровня защиты территориальных вод Иордании. Подтверждением этого сотрудничества и координации является обмен информацией с Центром морских операций, оснащенным самым современным оборудованием наблюдения и сложными сетями коммуникаций, и постоянное обновление планов обеспечения безопасности и реагирования на катастрофы применительно к району залива Акаба. Кроме того, мы находимся в постоянном контакте с офицерами безопасности и специализированными учреждениями, и проводим совместные морские учения на местном и национальном уровнях, где отрабатываются все возможные сценарии, повышающие стандарты межведомственной слаженности в работе и координации усилий.

«UNIPATH»: *Пожалуйста, расскажите о подготовке и обучении иорданских военных моряков и морских пехотинцев.*

Полковник Аль-Джарра: Все служащие ВМФ Иордании, включая офицеров, сержантов и старшин и другой личный состав, проходят обучение по интенсивной программе повышения квалификации и обучения, аналогичной программе подготовки в соответствии с базовыми требованиями ко всем военнослужащим. В эту программу входят такие дисциплины как первоначальная общая подготовка, обращение с оружием, снайперская стрельба, плавание, а также курс по вопросам безопасности и бдительности. За этим следует специализированная военно-морская и техническая подготовка, а также особая подготовка для морских пехотинцев в зависимости от особенностей их задач. Кроме того, наши моряки также проходят обучающие курсы в иорданских учреждениях, специализирующихся на военно-морских аспектах и вопросах безопасности, а также в гражданских институтах, специализирующихся на морских науках.

«UNIPATH»: *Проходит ли офицерский и сержантский состав обучение за пределами королевства?*

Полковник Аль-Джарра: Офицеры и сержанты ВМФ Иордании посещают целый ряд учебных курсов, организуемых союзными и дружественными странами в своих центрах обучения морскому делу. Сюда входят базовые курсы и курсы повышения квалификации для военных моряков в зависимости от выполняемых ими задач (моряки на военном судне, морские инженеры, водолазы, морские пехотинцы), а также курсы иностранных языков. Есть также учебные курсы для штабных офицеров и старших командиров, проводимые с целью повышения их эффективности и компетентности, а также с целью дать им новые навыки и знания, знакомя их с практикой их коллег из других стран.

«UNIPATH»: *Ставятся ли перед ВМФ Иордании задачи охраны морской экосистемы?*

Полковник Аль-Джарра: Одна из наиболее важных обязанностей иорданского ВМФ состоит именно в защите морской экосистемы. В Иордании создана специальная организация по защите водной окружающей среды, и постоянно осуществляется сотрудничество и координация усилий с тем, чтобы ее рекомендации относительно сохранения морской экосистемы и регулирования рыболовства претворялись в жизнь. Следует отметить, что ВМФ Иордании следит за индустрией рыбной ловли и запрещает нелегальные методы ловли рыбы. ✦

ЛИВАНСКИЙ ВАРИАНТ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Управление кибербезопасности Вооруженных сил Ливана повышает уровень информированности о возможных нападениях

Корреспондент журнала «Unipath» взял интервью у пресс-секретаря Вооруженных сил Ливана генерал-майора Али Кансо. Он рассказал, как военные Ливана борются с угрозами компьютерным сетям, которые могут негативно повлиять на национальную безопасность.

«Unipath»: Кибербезопасность стала составной частью национальной безопасности всех государств. С какими киберугрозами сталкивается Ливан?

Генерал-майор Кансо: Ливан испытывает киберугрозы со стороны многих субъектов, стремящихся взломать наши онлайновые системы, шпионить за нашими коммуникациями и похищать информацию. Есть террористические организации, которые взламывают аккаунты с целью пропаганды экстремистской идеологии среди молодежи и её вербовки. Также угрозу представляют отдельные люди или группировки в Ливане и в других странах, осуществляющие нападения на компьютерные сети правительств и их институтов.

Так что в этом контексте Ливан подвергается нападениям 24 часа в сутки, в том числе таким, как распределенный отказ в обслуживании и нападения на банковский сектор (с использованием вредоносных программ типа Gauss и Flame), сектор телекоммуникаций и различные гражданские компании.

Способность Ливана отражать такие атаки ослаблена отсутствием систем киберзащиты и обученных кадров, способных сдерживать подобные нападения. Как следствие, операции по обеспечению кибербезопасности ограничиваются мерами реагирования на уже совершившееся нападение и попытками защитить сети от таких нападений в будущем с привлечением всех имеющихся ресурсов.

«Unipath»: В чем состоит роль Управления кибербезопасности Вооруженных сил Ливана?

Генерал-майор Кансо: Для защиты своих ресурсов, имеющихся в рамках используемых ими систем и сетей, вооруженные силы большинства стран стремятся создавать управления кибербезопасности. Эти ресурсы включают в себя чувствительную информацию относительно безопасности и вооруженных сил страны и могут содержать данные о вооружениях, оборудовании, выполнении задач, размещении подразделений, а также личные и профессиональные данные военного и гражданского персонала. В эти ресурсы также входят сети Интранет, Интернет и беспроводные коммуникации.

Что касается Вооруженных сил Ливана, Управление кибербезопасности играет очень важную роль в сдерживании попыток нарушить работу систем, содержащих информацию о наших вооруженных силах и безопасности, или взломать их. Мы считаем это серьезной угрозой безопасности, создающей огромный риск для работы ливанской армии, ее подразделений и жизни военнослужащих.

«Unipath»: Насколько сильное влияние на ливанскую армию оказывают подобного рода нападения?

Генерал-майор Кансо: Вооруженные силы Ливана используют несколько систем киберсетей, в том числе официальные правительственные вебсайты, услуги электронной почты, приложения для смартфонов и другие. Они также обеспечивают доступ к Интернету для различных войск и подразделений.

Все эти системы могут служить объектами нападения со стороны врагов нашего государства или других сил, стремящихся нанести ущерб армии. Например, успешное нападение может привести к нарушению работы сети внутренних коммуникаций, которая обеспечивает связь подразделений с командованием. Могут быть взломаны веб-сайты армии или один из аккаунтов в официальных социальных сетевых ресурсах, может быть также похищена чувствительная информация из внутренней сети, в которой происходит обмен файлами.

Все это имело бы серьезные последствия для армии, ее подразделений и личного состава, особенно если похищенные данные попадут в руки террористических группировок, постоянными мишенями которых являются военнослужащие и места их расположения.

«Unipath»: Насколько важно международное сотрудничество в обеспечении защиты компьютерных сетей Ливана?

Генерал-майор Кансо: Международное сотрудничество в защите информационных сетей Ливана имеет критически важное значение. Сотрудничество осуществляется на двух уровнях: на первом уровне предоставляется современное программное обеспечение, необходимое для укрепления защиты сетей от кибератак, а на втором упор делается на человеческий фактор — осуществляется обучение специалистов методам своевременного и правильного реагирования на эти нападения с тем, чтобы предотвратить или минимизировать ущерб.

«Unipath»: Как вашим сотрудникам удается идти в ногу с постоянным развитием сферы кибербезопасности?

Генерал-майор Кансо: Наши военнослужащие проходят обучение на различных учебных курсах, слушают лекции и участвуют в конференциях как в Ливане, так и за границей. Цифровой мир идет вперед быстрыми шагами, и вредоносные программы для кибернападения ежедневно создаются тысячами. Кроме того, огромное количество группировок и отдельных лиц постоянно изобретают новые методы более изощренных кибератак. Наши противники также совершенствуют свои онлайновые возможности с целью проникновения в наши информационные системы.

Учитывая все это, наши сотрудники должны следить за последними разработками в сфере кибербезопасности с тем, чтобы быть готовыми принять новые вызовы. С другой стороны, укрепление нашей кибероборонны требует наличия сложного оборудования и компьютерных программ, которые мы получаем благодаря сотрудничеству с дружественными нам государствами и другими заинтересованными сторонами. ✦

РОЛЬ ЦЕНТРА МОРСКОЙ БЕЗОПАСНОСТИ ОМАНА

Слева направо: Генеральный директор Королевской полицейской береговой охраны Омана генерал-майор Али бин Саиф Аль Мукбали; контр-адмирал пакистанского ВМФ Абдул Муниб, бывший в то время командующим Объединенной тактической группой 151; и военный атташе Пакистана капитан Кашиф Фархан посещают штаб-квартиру Королевской полицейской береговой охраны Омана в г. Маскат.

Контр-адмирал Абдул Муниб, слева, и генерал-майор Аль-Мукбали обмениваются ценными подарками.

СОТРУДНИКИ ЖУРНАЛА «*UNIPATH*» | ФОТОГРАФИИ ОБЪЕДИНЕННОЙ ТАКТИЧЕСКОЙ ГРУППЫ 151

Центр морской безопасности, в котором работают сотрудники военных органов, органов безопасности и гражданских учреждений Омана, отвечает за безопасность и стабильность в территориальных водах страны.

Расположенный на территории гарнизона Аль-Муртафаа, центр получает доклады от всех этих ведомств и координирует свои действия с соответствующими органами. Специализированные системы и оборудование центра круглосуточно охраняют воды Омана.

Часть обязанностей центра включает:

1. Объединение усилий всех ведомств, отвечающих за морскую безопасность
2. Обеспечение необходимыми возможностями и ресурсами, такими как оборудование, приборы, разведывательные самолеты, суда и катера.
3. Разработку процедур и планов борьбы с незаконной деятельностью и организованной преступностью в портах, прибрежных сооружениях и на побережье.
4. Принятие необходимых мер и процедур по защите и сохранению рыбных запасов, природных ресурсов и морской флоры и фауны.
5. Реагирование на природные и гуманитарные катастрофы с задействованием всех имеющихся в распоряжении султаната возможностей и ресурсов.
6. Участие в планировании мер реагирования в случае кризисных ситуаций и природных катастроф на море и разработка возможных сценариев опасных ситуаций на море.
7. Повышение уровня осведомленности жителей страны и моряков о важности вопросов безопасности и сотрудничества в защите природных морских богатств султаната.
8. Отслеживание и наблюдение за движением судов в территориальных водах Омана и вблизи них.
9. Повышение уровня сотрудничества с союзными и дружественными странами, а также с региональными и международными организациями, занимающимися вопросами безопасности на море.

В обязанности центра также входит отслеживание нарушений в территориальных водах Омана и вблизи них. К таким нарушениям относятся:

1. Морское пиратство
2. Незаконная миграция или проникновение на территорию страны
3. Незаконное рыболовство и чрезмерный вылов рыбы
4. Загрязнение морских вод
5. Создание препятствий на международных морских маршрутах
6. Терроризм на море
7. Вмешательство в работу прибрежных нефтяных сооружений и диверсии против них
8. Организованная преступность, незаконная торговля и контрабандные операции ✦

Контр-адмирал Абдул Муниб, в центре, и личный состав его штаба осматривают Центр морской безопасности Омана.

Энергичный лидер

Генерал-полковник Каис Халаф Рахима противостоит старым и новым угрозам

СОТРУДНИКИ ЖУРНАЛА «UNIPATH» | ФОТОГРАФИИ: МИНИСТЕРСТВО ОБОРОНЫ ИРАКА

Его цвет кожи и ярко выраженные черты лица свидетельствуют о его сумерских корнях. Это добродушный, отважный и вежливый человек, обращаясь к своему гостю, он выбирает изысканные слова в духе южного гостеприимства. Его скромность и вежливое обращение отнюдь не мешают ему овладевать военными науками. Как военный, участвовавший во многих сражениях, он создал себе репутацию целеустремленного и готового к самопожертвованию бойца, который думает только о победе.

Мы говорим о генерал-полковнике Каисе Халафе Рахима, заместителе начальника штаба иракской армии по оперативным вопросам и командующим Командования совместными операциями в Ираке. Это человек-легенда, который много значит для политического руководства и сил безопасности страны. Его профессионализм и целостность характера убеждают нас в том, что он способен достойно выполнить трудную задачу по защите страны.

Он родился в г. Майсан в 1962 г., с ранних лет научился манере ведения беседы между порядочными людьми. В 1984 г. он окончил Первое военное училище, получил степень магистра после первой войны в Арабском заливе, а докторскую степень после освобождения Мосула, когда свои научные исследования он подкрепил боевым опытом.

«Когда я поступил в военное училище в 1984 г., ирано-иракская война была в своей наиболее интенсивной фазе, - вспоминает генерал. – Училище было своеобразной линией фронта, где курсанты получали знания от своих преподавателей, возвратившихся с передовой для того, чтобы передать нам свой опыт и уроки, полученные в боях. Мы многому научились у полевых командиров, которые читали нам лекции. После окончания училища у нас были академические знания и практический опыт, как будто бы мы действительно принимали участие в боевых действиях».

Хотя он работал в сфере оперативных направлений, генерал-полковник Каис стремился получить знания и в области стратегических исследований, для чего в 2010 г. поступил в Национальное военное училище.

«Я был очень рад, что Министерство обороны направило меня на изучение [национальной стратегии безопасности] и получение степени магистра. Обучение имело уникальный характер, курсы нам читали преподаватели, которые были специалистами в области политических и военных наук. Это был уникальный опыт еще и потому, что я получал практические знания непосредственно в Тал Афар, и параллельно с освоением учебной программы я начал анализировать планы, которые я составил для восстановления безопасности в этом городе. Это подтолкнуло меня в 2019 г. к идее написания диссертации на соискание докторской степени на тему «Новые войны и трансформация в концепции силы». Несмотря на то, что я продолжал работать в должности оперативного командира в среднем районе реки Евфрат, а также несмотря на условия безопасности в моей стране и неоднократные перерывы в работе над диссертацией, я был настроен довести свое исследование до конца. Тем более, что тема исследования напрямую связана со всеми трудностями, которые переживает Ирак, особенно с войной пятого и шестого поколения».

Генерал-полковник Каис не остановился на изучении традиционных форм ведения войны. Он взял на себя инициативу погружения в мир современной военной науки, проводя стратегические исследования и осознавая важность и опасность таких аспектов как кибервойны и доминирование террористических и экстремистских группировок в социальных СМИ.

«После всех бед, которые принесла Даиш на захваченных ими обширных территориях, эта организация сделала

ставку на психологическую войну, начав распространять слухи в социальных сетях, чтобы еще больше усугубить ситуацию с безопасностью. На том этапе государственные, официальные и неофициальные медийные институты не были в состоянии принять адекватные ответные меры. Террористические группировки действовали на огромном оперативном пространстве и вселяли ужас в сердца людей, совершая обезглавливания, взрывая рынки, захватывая женщин и выставляя все эти кадры на страницах социальных сетей в качестве посланий остальным, - говорит генерал. – Их целью было сломать боевой дух наших бойцов и заставить мирных жителей подчиниться, а силы безопасности сдаться. Мы начали с того, что стали разрушать их киберсети, работающие за пределами Ирака и на контролируемых террористами территориях».

Генерал и его коллеги действовали совместно с силами международной коалиции для того, чтобы обнаружить и обезвредить сети, которые Даиш использовала в кибервойне. Группы иракских специалистов-электронщиков также сотрудничали со специалистами из сил коалиции с целью отследить тех, кто выставлял твиты и блоги в поддержку Даиш, и закрыть их аккаунты.

«Затем мы основной упор сделали на восстановление уверенности в себе и поднятие боевого духа наших военных, и нам удалось восстановить психологическую боевую готовность личного состава наших подразделений, - отметил генерал. – Как следствие этого, наши героические воины показали себя на поле боя, ни разу не покинули свой сектор ответственности, даже в самых ожесточенных сражениях. Они стали понимать, что представления, созданные онлайновой пропагандой Даиш – будто террористы были воинами с другой планеты, которых пули не берут и которых победить невозможно – оказались большой ложью».

Генерал признает, что социальные СМИ и молодежь внесли вклад в победу над Даиш. Они разоблачали ложь Даиш, и террористам становилось все труднее распространять дезинформацию. Именно таким образом электронная армия и медийная машина Даиш проиграли войну гражданским активистам, агентам разведки и силам коалиции, которые проложили путь к поражению Даиш на поле боя.

Танк M1A1 9-ой бронетанковой дивизии Ирака занимает оборонную позицию на окраине Мосула в 2017г.

Признавая тот факт, что войны четвертого, пятого и шестого поколений опираются на современные технологии, генерал-полковник Каис советует армиям идти в ногу с технологическим развитием с тем, чтобы они могли противостоять нынешним и будущим угрозам, которые обычно относятся к категории асимметричных войн. Армии должны укреплять свою оборону в режиме онлайн и создавать ведомства, ответственные за киберразведку и способные отслеживать деятельность противника и предотвращать взломы систем национальной безопасности и проведение кибернападений злоумышленными группировками. Генерал отмечает, что современные технологии, интернет и беспилотники усложняют работу служб безопасности.

В 2004-2008 гг. генерал-полковник командовал 10-й бригадой в районе Тал Афар, который был очагом деятельности Аль-Кайды, толкавшей Ирак в опасном направлении. В городах там господствовали террористические банды и враждовавшие между собой сектарианские группировки.

«На меня возложили сложную задачу и ответственность по ряду причин, в основном, потому что Аль-Кайда контролировала город и прилегающие районы, а также из-за демографических особенностей населения, состоявшего из многочисленных этнических и религиозных групп, - вспоминает генерал. – Я принял командование 10-й бригадой в те дни, когда на лице каждого иракца были написаны страх и отчаяние, и угроза смерти витала над их головами. Полицейская служба еще не была сформирована, что возлагало еще большие тяготы на плечи армии в вопросах обеспечения безопасности. Силы безопасности, которые не смогли защитить город от террористических актов, в значительной степени утратили доверие населения. Благодаря слаженной работе с силами коалиции ситуация начала постепенно стабилизироваться. Основной упор был сделан на обеспечение безопасности и на разведку, которая полагалась на гражданские и национальные источники информации и старалась стабилизировать ситуацию в городе. Также были призывы к суннитскому населению Тал Афар вступить

Танк M1A1 9-ой бронетанковой дивизии Ирака вступает в бой за Мосул в 2017г.

в ряды армии и полиции, и позднее это стало одной из наиболее важных целей, которых нам удалось достичь. Мы старались снизить религиозные и этнические различия в местных судебных органах, внушить уверенность, отвергать сектарианскую враждебность и наладить диалог с населением».

В начале октября 2019 г. в Багдаде произошло кровопролитие, когда против демонстрантов, требовавших улучшения экономических условий и искоренения коррупции в правительственных органах, недисциплинированными представителями правоохранительных органов была применена чрезмерная сила, что могло ввергнуть Ирак в пучину хаоса. У военно-политического руководства страны не было иного выбора, кроме как сменить руководителей сил безопасности в этих районах, а командующим назначить офицера, обладающего такими качествами как сдержанность, патриотизм и отвага. Именно в это время и было принято решение поручить эту трудную задачу генерал-полковнику Каису.

«Большое количество жертв среди мирного населения вызвало серьезный раскол доверия между жителями и силами безопасности, а неясна картина безопасности еще больше усложняла ситуацию. Большую проблему представляло отсутствие специализированных подразделений, обученных и оснащенных для выполнения таких заданий. Конечно же, такие особые задания и обязанности требуют мудрости, патриотизма, выдержки и сострадания, а уж потом только военного опыта и лидерского искусства. Помимо этого, необходимо было завоевать доверие мирных демонстрантов, защищая их и не позволяя силам безопасности спровоцировать их».

Было также необходимо действовать в рамках Конституции и других законов, регулирующих борьбу с беспорядками и агрессивно настроенными демонстрантами, которые наносили ущерб инфраструктуре и сферам безопасности и сильно отличались от мирно протестующих в соответствии с положениями Конституции.

«Как только я вступил в должность, я четко очертил круг ответственности каждого подразделения, определил юрисдикцию каждого офицера и четкие ограничения с целью соблюдения международных договоров по правам человека и разделения демонстрантов и сил безопасности, - пояснил генерал. – На заградительных барьерах и контрольно-пропускных пунктах были установлены камеры для регистрации любых нарушений дисциплины. Я отдал четкие приказы и взял с каждого офицера подписку об отказе от использования боевых патронов против демонстрантов при любых обстоятельствах, я также предотвратил использование резиновых пуль и слезоточивого газа».

Он ежедневно общался с мирными активистами и демонстрантами, что привело к быстрой стабилизации ситуации.

«Мы восстановили уважение к армии и к силам безопасности, - говорит генерал. – В конце концов, их назначение именно в защите людей, и они черпают свою силу и целеустремленность именно у них».

Слева: Группа министерства обороны Ирака по наблюдению за СМИ отлеживает вещание для реагирования на террористическую пропаганду.

Справа: Генерал-полковник Каис, бывший в то время командующим по оперативному планированию в Багдаде, разговаривает с активистом на площади Тахрир в 2019 г.

Ливан усиливает электронное наблюдение в борьбе с контрабандными операциями

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

С целью «залатать бреши» в механизмах обеспечения безопасности вдоль границы с Сирией, Вооруженные силы Ливана привели в действие систему наблюдения, охватывающую всю страну.

Контрабандные операции и незаконное проникновение в страну стали настолько серьезной проблемой, что с 2009 г. Ливан был вынужден постоянно держать на своих северных и восточных границах четыре полка.

Для того, чтобы перекрыть пути для ввоза контрабанды, армия также создала сеть вышек электронного мониторинга, связанную с Центром совместных операций и информации при Командовании Вооруженными силами Ливана. Эта система позволяет проводить круглосуточное наблюдение, передавая сигналы раннего оповещения мобильным подразделениям, ответственным за перехват нарушителей. Об этом заявил глава Объединенного комитета обеспечения безопасности границ Ливана генерал Джозеф Хаддад.

Второй этап плана, начавшийся в ноябре 2021 г., состоит в интегрировании береговых радаров наблюдения в сеть наземных вышек наблюдения. По словам генерала Хаддада, такая интегрированная система «обеспечивает раннее оповещение в кризисных ситуациях».

1-й полк наземной пограничной службы ливанской армии действует в районе от Средиземного моря до г. Вади Халед. 2-й полк наземной пограничной службы отвечает за верхнюю половину границы с Сирией в районе Баалбек-Хермел. 3-й полк действует в горном районе возле г. Рашайя, а зона ответственности 4-го полка охватывает нижнюю половину границы в районе Баалбек-Хермел.

AFP/GETTY IMAGES

Бойцы сил безопасности Ливана на погранпереходе на границе с Сирией в г. Эль-Каа.

Стремление Ливана обезопасить свои границы встретило поддержку со стороны международных партнеров. Посол Великобритании в Ливане Иан Коллард, посол США Дороти Шей и посол Канады Шантэл Шастеней встретились в ноябре 2021 г. с командующим Вооруженными силами Ливана Джозефом Аоуном для обсуждения вопросов безопасности на ливанско-сирийской границе.

«Дискуссии были сосредоточены на задаче Вооруженных сил Ливана обеспечить безопасность всей ливано-сирийской границы и на трудностях, с которыми сталкивается армия из-за многочисленных проблем в стране», - говорится в заявлении посольства Великобритании.

Во время встречи посол Коллард объявил о безвозмездной помощи в размере 1,4 млн. долл. США для повышения жизнестойкости ливанской армии с предоставлением запасных частей для Ленд Роверов, ранее бесплатно переданных Великобританией, и средств персональной защиты для военнослужащих-женщин, участвующих в операциях в приграничных районах.

Эта помощь Великобритании последовала за сделанным в сентябре 2021 г. заявлением США о предоставлении военной помощи Ливану в размере 47 млн. долл. США.

Выступая с брифингом перед Советом Безопасности ООН в ноябре 2021 г., специальный координатор ООН по Ливану Иоанна Вронецка призвала к оказанию дополнительной международной поддержки Вооруженным силам Ливана и отметила важную роль, которую играет ливанская армия в обеспечении безопасности и стабильности страны.

Источники: Канцелярия специального координатора ООН по Ливану, defensenews.com, arabweekly.com

Кыргызстан активно проводит внутренние реформы

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Кыргызстан использует материальную помощь Европейского союза для поддержки правительственных реформ, инициатив по правам человека, а также для обеспечения водоснабжения.

В декабре 2021 г. Европейский союз одобрил финансирование в размере 62 млн. евро в рамках четырехгодичной программы помощи Кыргызстану.

В том, что касается реформы управления и перехода на цифровые технологии, финансирование в основном будет направляться на пропаганду и совершенствование механизма обеспечения верховенства закона и внедрение цифровых платформ.

Президент Кыргызстана Садыр Джапаров вместе с супругой Айгуль Асанбаевой на избирательном участке во время парламентских выборов. Бишкек, ноябрь 2021 г.
AFP/GETTY IMAGES

Помощь Бишкеку со стороны ЕС также охватывает и аспекты человеческого фактора, такие как улучшение качества образования и обеспечение гендерного равенства и прав человека.

ЕС также подчеркнул необходимость для Кыргызстана в интегрировании и совместном использовании водных ресурсов в пределах этого полузасушливого региона. Вопрос обеспечения безопасности водоснабжения остается предметом серьезных дипломатических переговоров между странами Центральной Азии еще со времен распада Советского Союза.

Эти приоритетные направления финансирования были определены в ходе консультаций между Кыргызстаном и странами-членами ЕС. Эти приоритеты также находятся в соответствии с Повесткой дня ООН до 2030 г., Парижским соглашением по климату и Глобальной стратегией ЕС.

«У ЕС сложились давние отношения с Республикой Кыргызстан как с ведущим и надежным партнером по развитию, - подчеркнул после подписания соглашения о финансировании в конце 2021 г. глава посетившей Кыргызстан делегации ЕС посол Эдуард Ауэр. – Сегодня мы отмечаем новый шаг в нашем сотрудничестве и принимаем на себя обязательства по долгосрочной поддержке в таких областях как государственное управление, цифровые технологии, образование, охрана окружающей среды и в других сферах, представляющих взаимный интерес. Новая многоступенчатая программа является убедительным доказательством постоянной поддержки, оказываемой народу Кыргызстана со стороны ЕС». **Источники: «Вечерний Бишкек», Vesti.kg**

ТУРКМЕНИСТАН объявил свои внешнеполитические цели

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Во время своего выступления перед Генеральной Ассамблеей ООН 21 сентября 2021 г. президент Туркменистана Гурбангулу Бердымухаммедов выразил приверженность своей страны миру, безопасности и дипломатическому разрешению споров.

Президент Бердымухаммедов объявил о том, что его страна проведет в Ашгабаде в декабре 2021 г. международную конференцию под названием «Политика мира и доверия – основа международной безопасности, стабильности и развития».

В своем выступлении в ООН он также предложил создание зоны мира, доверия и сотрудничества с названием «Центральная Азия – Каспийский регион». Он подчеркнул, что Туркменистан заинтересован в установлении мира, гармонии и единства в Афганистане и способствует достижению этой цели.

В заключительной части своего выступления президент Бердымухаммедов подтвердил готовность Туркменистана к ведению диалога по вопросам достижения целей устойчивого развития, включая усилия по сведению к минимуму последствий опустынивания земель вблизи Аральского моря. Он выразил готовность разработать совместно с региональными партнерами специальную программу ООН для бассейна Аральского моря.

Источники: Turkmenportal, Организация Объединенных Наций

Хуситы обвиняются в казнях мирных жителей

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Легитимное правительство Йемена выразило протест в связи с незаконной казнью девяти человек, в том числе 17-летнего подростка, которых хуситы обвинили в убийстве одного из своих лидеров.

После того, как эти девять человек были обвинены в причастности к смерти Салеха аль-Самада в 2018 г., они были незаконно задержаны и подверглись пыткам и другим издевательствам.

Предупреждая население о том, что повстанцы-хуситы будут и дальше прибегать к массовым убийствам невинных мирных граждан, министр информации Йемена Муаммар Аль-Ирьяни назвал внесудебные казни спланированным убийством на основании сфабрикованных обвинений.

Аль-Самад и еще шестеро повстанцев были убиты в ходе воздушного нападения, осуществленного Коалицией по восстановлению законности в Йемене. Являясь председателем Верховного совета хуситов, Аль-Самад был одной из наиболее влиятельных политических фигур в этой группировке.

Региональные социальные медийные платформы опубликовали имена и фотографии казненных йеменцев: Али Аль-Кузи, Абдул-Малик Хамид, Мухаммад Хаиг, Мухаммад Аль-Кузи, Мухаммад Нох, Ибрагим Акель, Мухаммад Аль-Машхари, Абдул-Азиз Аль-Асвад и Моаз Аббас. Все они проживали в районе Аль Канавис в провинции Аль Ходейда.

Организации по защите прав человека, такие как Йеменская коалиция по мониторингу нарушений прав человека, SAM для борьбы за права и свободы, Радар прав человека, Ассоциация матерей похищенных детей и Национальная ассоциация по защите прав и свобод выпустили совместное заявление, резко осуждающее совершенные хуситами казни.

Восьмилетний конфликт разорил Йемен, принес неисчислимые страдания его народу и согнал с родных земель более 4 млн. его граждан. С начала гражданской войны в сентябре 2014 г. в стране погибло более 233 тыс. человек, в том числе 102 тыс. человек в результате непосредственных боевых действий и еще 131 тыс. от вторичных причин, таких как голод и плохое медицинское обслуживание.

Серьезные нарушения международного гуманитарного права и вопиющие нарушения прав человека, совершаемые повстанцами-хуситами, еще больше усугубили самый масштабный в мире гуманитарный кризис, вызванный действиями самих людей. Более того, препятствия, воздвигаемые хуситами на маршрутах доставки гуманитарной помощи, способствуют распространению заболеваний, в том числе эпидемии холеры и COVID-19.

Источники: Си-Эн-Эн, Alhurra, Al Jazeera

Диалог и дипломатические переговоры между Узбекистаном и США

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

В декабре 2021 г. Узбекистан организовал первую встречу в рамках Диалога стратегического партнерства с США, на которой основное внимание было уделено обязательствам двух стран по укреплению безопасности в Центральной Азии.

Сопредседателями на встрече были министр иностранных дел Узбекистана Абдулазиз Камилов и помощник госсекретаря США по региону Южной и Центральной Азии Дональд Лу.

Министр иностранных дел Узбекистана Абдулазиз Камилов, слева, встречается в Вашингтоне с госсекретарем США Энтони Блинкеном. 2021 г. AFP/GETTY IMAGES

Обе стороны подчеркнули важность продолжения сотрудничества для борьбы с угрозами терроризма и экстремизма и стабилизации ситуации в Афганистане. Решение властей Узбекистана разрешить пользоваться грузовым терминалом в Термезе для содействия в доставке гуманитарной помощи в Афганистан было с благодарностью встречено американской стороной.

Управление Верховного комиссара ООН по делам беженцев и Всемирная продовольственная программа ООН использовали транспортный узел в Термезе для поставок в Афганистан продовольствия, палаток, посуды, одеял и других необходимых предметов.

Вашингтон согласился организовать в США следующую встречу в рамках Диалога стратегического партнерства. Встреча в 2022 г. может совпасть с 30-й годовщиной установления дипломатических отношений между Узбекистаном и США.

За шестилетний период пребывания у власти президента Узбекистана Шавката Мирзиёева двусторонние отношения заметно улучшились и сейчас включают более широкое военное сотрудничество и обучение.

Источники: Агентство «Анадолу», Газета.uz, Каравансарай

ОАЭ ВЫСТУПАЮТ ЗА УКРЕПЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Компания «Majid Al Futtaim Retail» из Объединенных Арабских Эмиратов, являющаяся одной из крупнейших сетей супермаркетов в регионе Ближнего Востока, Южной Азии и Северной Африки, удостоилась высокой похвалы за внедрение передового опыта в сфере кибербезопасности.

В ходе Выставки информационных технологий стран Арабского залива – торгово-промышленной ярмарки потребительских товаров, проведенной в Дубае в октябре 2021 г., сеть «Majid Al Futtaim» была особо отмечена фирмой «Trend Micro Inc.» за её усилия в обеспечении компьютерной безопасности в сотнях своих продуктовых магазинов. Компания «Majid Al Futtaim» является франчайзополучателем и оператором сети «Carrefour», головной офис которой находится во Франции.

Представитель «Trend Micro» отметил, что «Majid Al Futtaim» отвечает за защиту от хакеров и преступников более 10 тыс. компьютеров, ноутбуков и мобильных устройств и 2 тыс. 500 серверов.

«За последние пять лет «Majid Al Futtaim Retail» добилась потрясающих успехов в переходе на цифровые платформы … Мы вместе прошли этот путь, и для нас это большая честь», - отметил вице-президент и управляющий директор «Trend Micro» д-р Моатаз бин Али.

Созданная Маджидом Аль Футаимом в 1992 г. и названная его именем, эта холдинговая компания со штабквартирой в Дубае помимо бизнес-отношений с компаний «Carrefour» также управляет большими торговыми центрами и развлекательными заведениями.

«Trend Micro Inc.» – американо-японская многонациональная корпорация, специализирующаяся на программном обеспечении в сфере кибербезопасности. Головные офисы компании находятся в Токио, Япония, и в г. Ирвинг, штат Техас, США.

Осознавая возрастающие по всему миру угрозы кибербезопасности, ОАЭ предпринимают значительные упреждающие усилия, чтобы быть готовыми противостоять этим угрозам. Советник правительства ОАЭ по вопросам кибербезопасности д-р Мухамед Аль-Кувеити в ходе Международного форума по вопросам правительственных коммуникаций, проведенном в сентябре 2021 г. в г. Шарджа, призвал к бдительности.

Аль-Кувеити выступил за обмен информацией между национальными рабочими группами, отвечающими за кибербезопасность для того, чтобы поднять уровень информированности людей о необходимости защищать цифровые устройства в государственном и частном секторе. Международный форум правительственных коммуникаций, на котором в 2021 г. присутствовало 79 экспертов из 11 стран, высказался за расширение обмена знаниями и стратегическими решениями в целях усиления защиты быстро развивающихся глобальных коммуникаций.

Источники: Агентство «Emirates», «Al-Ittihad», Zawya.com

Силы безопасности Пакистана демонстрируют рекордное количество героина, перевезенного в тайнике из Афганистана через пограничный пункт Торхам.
AFP/GETTY IMAGES

Пакистан и США конфисковали тонны запрещенных наркотиков, ввезенных из Афганистана

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Правительство Пакистана сообщило о конфискации рекордного количества запрещенных наркотиков на одном из основных контрольно-пропускных пунктов на границе страны с Афганистаном.

Всего лишь за несколько недель в декабре 2021 г. и январе 2022 г. пакистанские власти на пограничном пункте Торхам предотвратили контрабандный ввоз в страну 524 килограммов гашиша, 255 килограммов героина, 280 килограммов опиума и почти 22 килограммов метамфетамина.

6 января 2022 г. органы Пакистана обнаружили два отдельных тайника с героином – в одном было 100 килограммов наркотика, а в другом 130 килограммов. Эта последняя конфискация стала рекордной для пункта Торхам. Действуя по наводке, пакистанцы обнаружили спрятанный в грузовике героин в терминале импортных поставок в Торхаме. Об этом сообщил глава таможенного отдела в Пешаваре Ахмад Раза Хан.

Пакистанская Служба по борьбе с наркотиками также захватила большое количество запрещенных наркотиков по всей стране. В конце декабря эта служба объявила о перехвате 2,2 тонн наркотиков, включая героин и метамфетамин, за чем последовала конфискация более 3 тонн наркотиков в первой половине января.

Наркотики прибывают из Афганистана в «огромных количествах», замечает сотрудник Отдела акцизов, налогообложения и контроля за наркотиками провинции Хибер Пахтунхва Азлан Аслам. Контрабандные перевозки возрастают, несмотря на обещания недавно пришедшего к власти в Афганистане правительства Талибана бороться с нелегальной наркоторговлей.

Афганистан по-прежнему остается источником почти всего распространяемого в мире опиума и героина. На его долю также приходится значительная часть производства метамфетамина и гашиша. Количество тайников с наркотиками из Афганистана в Иране, Юго-Восточной Европе и Турции постоянно множится.

В декабре 2021 г. ВМФ США захватил 385 килограммов героина на иранском судне в Аравийском море. Двумя неделями ранее американское патрульное судно спасло пятерых иранских матросов с горящего дау в Оманском заливе. Иранцы пытались сжечь следы своей преступной деятельности, но американским военным морякам удалось конфисковать оставшиеся 1 тыс. 750 килограммов гашиша, 500 килограммов метамфетамина и 30 килограммов героина.

Источники: TRT World, Военно-морской флот США, «Daily Pakistan»

Вооруженные силы Омана противостоят циклону Шахин

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Превентивные меры, принятые Вооруженными силами султаната в октябре 2021 г., спасли жизни, возможно, сотен оманцев, проживающих на траектории движения циклона Шахин.

Когда на страну обрушился ураган со скоростью ветра до 150 километров в час и высотой волн до 10 метров, власти Омана спасли более 600 человек.

Люди пробираются по затопленным улицам в г. аль-Муссанах на севере Омана после того, как на регион обрушился циклон Шахин. Октябрь 2021 г.
AFP/GETTY IMAGES

Для того чтобы снизить число возможных жертв надвигающегося циклона, Служба внутренней безопасности Омана остановила дорожное движение в провинциях Аль Батина Север и Аль Батина Юг, разрешив движение только автомобилям служб экстренной помощи и доставки жизненно важных товаров. Также во избежание несчастных случаев было отключено электричество в восточном пригороде Маската аль-Курм, а более чем 2 тыс. 700 жителям помогли укрыться в убежищах.

На время циклона власти Омана дали государственным служащим неоплачиваемый отпуск и приостановили прием и отправку рейсов в международном аэропорту Маската. В районе Аль-Хабура к северо-западу от столицы страны Маскат дождевые осадки достигли 369 миллиметров.

Его Величество султан Хайтам бин Тарик создал министерский комитет для оценки имущественного ущерба, нанесенного циклоном. Не остались в стороне и дружественные Оману страны в регионе. После телефонного звонка заместителя премьер-министра Омана по вопросам обороны Шихаба бин Тарика Кувейт направил в Оман военные ресурсы.

Его Величество король Иордании Абдулла II ибн Аль Хуссейн позвонил султану Хайтаму бин Тарику и выразил соболезнование и сочувствие, тем самым продемонстрировав поддержку народу Омана. **Источники: Би-Би-Си, Рейтер, alkhaleejonline**

СТРАТЕГИЧЕСКОЕ ПАРТНЕРСТВО КАЗАХСТАНА С США

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

В рамках расширяющегося партнерства в сфере дипломатии и безопасности дипломаты высокого ранга из Казахстана и Соединенных Штатов выразили приверженность своих стран дальнейшему сотрудничеству в вопросах борьбы с терроризмом, нераспространения ядерного оружия и укрепления безопасности границ.

В декабре 2021 г. в столице Казахстана г. Астана прошла встреча заместителя министра иностранных дел Казахстана Акана Рахметуллина и помощника госсекретаря США по региону Южной и Центральной Азии Дональда Лу.

От имени США Лу выразил благодарность Казахстану за его эффективное сотрудничество по таким вопросам как безопасность границ, борьба с терроризмом, миротворческие операции, нераспространение ядерного оружия, изменение климата и региональная безопасность.

Он дал высокую оценку ведущей роли Казахстана в репатриации иностранных боевиков и их семей из зон вооруженных конфликтов и пообещал и дальше продолжать двустороннее сотрудничество в вопросах реабилитации и реинтеграции этих людей.

Обе стороны подчеркнули глобальное лидерство Казахстана в сдерживании распространения ядерного оружия. Американская сторона еще раз подтвердила свое долгосрочное обязательство по оказанию помощи Казахстану в уничтожении радиоактивных отходов с ядерного полигона в Семипалатинске, оставшихся с тех времен, когда в регионе доминировала Москва.

Оба дипломата выразили поддержку углубляющимся отношениям между военными, пограничниками, таможенниками и правоохранительными органами двух стран. Эта поддержка будет осуществляться посредством выполнения четвертого пятилетнего плана военного сотрудничества между министерствами обороны Казахстана и США.

Источники: Baige News, Голос Америки

Саудовская военнослужащая Абир Абдулла аль-Рашед на пресс-конференции, на которой обсуждались вопросы безопасности во время ежегодного паломничества в Мекку. РЕЙТЕР

Женщины Саудовской Аравии с гордостью вступают в ряды Вооруженных сил

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

В сентябре 2021 г. состоялось историческое событие: Центр подготовки женских кадров личного состава Вооруженных сил Саудовской Аравии после 14 недель тренировок выпустил первую группу саудовских женщин-военнослужащих.

«Ежедневная программа обучения начинается с утренней проверки, потом следует период физической подготовки под руководством фитнес-тренеров, затем у курсанток перерыв на завтрак, после чего они приступают к полевым занятиям. После их окончания начинаются теоретические занятия», - поясняет инструктор Манахил бинт Салех бин Хумаид.

О плане разрешить саудовским женщинам служить в армии было объявлено в 2019 г., хотя впервые женщины-военнослужащие появились на публике только в июле 2021 г. в качестве охранников во время паломничества в Мекку.

«Одна из причин, почему я вступила в Вооруженные силы, это появляющееся у меня чувство безопасности, когда я вижу мужчин в форме, охраняющих общественные места и обеспечивающих безопасность, - говорит одна из выпускниц курса. – И поэтому, когда у меня появилась возможность внести свой вклад в обеспечение этого ощущения безопасности, то я времени зря не теряла».

На выпускной церемонии с речью выступил начальник Управления обучения и воспитания Вооруженных сил Саудовской Аравии генерал-лейтенант Адель бин Мухаммед Аль-Белви, в которой он сделал краткий обзор работы Центра подготовки женских кадров личного состава.

Одобренный в Саудовской Аравии документ «Видение на период до 2030 г.» включает установление в стране гендерного равенства. Саудовские ответственные работники постановили, что принципы современных прав женщин не вступают в противоречие с правами, гарантированными исламскими законами.

В качестве еще более амбициозного начинания, в 2018 г. королевство ввело в Управлении общей безопасности, Министерстве внутренних дел и в семи из 13 регионов страны: Рияд, Мекка, аль-Кассим, аль-Мадина, Ассир, Аш-Шаркия и Аль-Баха должности для женщин. С тех пор число работающих там женщин возросло.

Источники: Си-Эн-Эн, Al Jazeera, Рейтер

Кувейт рассматривает возможность набора на военную службу женщин

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Стремясь увеличить число военнослужащих в стране, Вооруженные силы Кувейта изучают положительные стороны принятия в свои ряды женщин. Заместитель начальника штаба по личному составу генерал-лейтенант Халед Аль-Кандари объявил, что анализ перспектив приема женщин на военную службу должен завершиться к концу 2021 г.

Споры насчет призыва женщин в армию возродились в сентябре 2021 г. в ходе призывной кампании под названием «Будь одной из них», начатой Министерством обороны Кувейта.

Подобную инициативу Кувейт рассматривал и в 2018 г., когда шейх Нассер Аль Сабах, бывший в то время министром обороны, выступил в защиту призыва женщин на военную службу. «Если женщины захотят поступить на национальную военную службу, то нет никаких возражений», - заявил тогда шейх Нассер.

Женщины уже служат в других органах безопасности Кувейта, однако вооруженные силы пока остаются исключением. В 2008 г. начали готовить женщин-полицейских, когда в первую группу курсантов набрали 40 женщин. В 2016 г. первые пять женщин-полицейских присоединились к силам безопасности в качестве охранников в Национальной Ассамблее Кувейта.

Усилия стран Персидского залива по расширению возможностей женщин медленно, но верно набирают обороты по мере того, как женщины начали занимать должности в ведомствах безопасности и обороны, которые ранее считались исключительной прерогативой мужчин.

Младший лейтенант Сара Аль-Сарраф стоит на посту у здания Национальной Ассамблеи Кувейта. AFP/GETTY IMAGES

Более 30 лет назад Силы обороны Бахрейна разрешили женщинам служить в некоторых родах войск, и некоторые из них дослужились до высоких чинов. В 2009 г. произошло историческое событие, когда две женщины-военнослужащие стали выпускницами Программы командования и генерального штаба при Королевском командно-штабном училище национальной обороны Бахрейна; после выпуска они стали штабными офицерами.

В Объединенных Арабских Эмиратах в 1991 г. открылось Военное училище для женщин им. Хавлы Бинт Аль Азвара, первое училище такого рода в регионе Персидского залива. В Катаре в 2018 г. женщинам было разрешено поступать на национальную службу в качестве добровольцев. **Источники: Al Jazeera, Al Hurra**

ТАДЖИКИСТАН И УЗБЕКИСТАН: ПОБЕДИТЬ ТЕРРОРИЗМ МОЖНО ТОЛЬКО СОВМЕСТНЫМИ УСИЛИЯМИ

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Стремясь повысить уровень региональной безопасности в Центральной Азии, парламент Таджикистана ратифицировал соглашения с Узбекистаном о сотрудничестве в таких областях как противовоздушная оборона и военная разведка.

Эти соглашения были подписаны в ходе официального визита в Таджикистан президента Узбекистана Шавката Мирзиёева в июне 2021 г., но окончательное одобрение в Таджикистане получили только в декабре 2021 г.

В том, что касается воздушных сил противовоздушной обороны, две стороны договорились об обмене передовым опытом в этой области, о проведении совместных учений, об оказании взаимной помощи терпящим бедствие самолетам и об обмене информацией о воздушном движении.

Обмен разведывательными данными в основном предполагает обмен информацией о подозреваемых террористах и религиозных экстремистских группировках. Будет передаваться информация о спонсорах и соучастниках террористов, а также о вооружении, тренировочных лагерях и базах террористов.

Таджикистан и Узбекистан также договорились предупреждать друг друга о повышенных террористических угрозах, включая угрозы суверенитету и территориальной целостности каждой из стран. Еще более углубляя сотрудничество, соглашение предусматривает проведение совместных военных учений боевых и разведывательных подразделений.

Третье соглашение разрешает в случае бедствий и чрезвычайных ситуаций использовать воздушное пространство и аэродромы друг друга и оговаривает механизм пересечения воздушного пространства другой стороны экипажами воздушных судов каждой из стран. Это соглашение заключено на пятилетний строк.

После того, как Мирзиёев стал президентом в 2016 г., дипломатические отношения и контакты в сфере безопасности между Таджикистаном и Узбекистаном существенно расширились.

Источники: Asia Plus, Eurasia Daily, «Свободная Европа»/Радио «Свобода»

ИРАКЦЫ ОБЕСПЕЧИВАЮТ БЕЗОПАСНОСТЬ ПАРЛАМЕНТСКИХ ВЫБОРОВ

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Сотрудники Высшей независимой избирательной комиссии Ирака подсчитывают бюллетени на парламентских выборах. Багдад, октябрь 2021 г.
AFP/GETTY IMAGES

Совместные усилия сотен тысяч иракских полицейских и военных помогли обеспечить безопасность досрочных парламентских выборов, проведенных в стране в октябре 2021 г.

Несмотря на то, что комендантский час не вводился, как во время предыдущих выборов, в стране не было ни террористических нападений, ни несчастных случаев, ни нарушений требований безопасности. Об этом заявило Министерство внутренних дел Ирака.

План обеспечения безопасности выборов включал задействование 300 тыс. военнослужащих, полицейских, служащих ВВС, Военной авиации и гражданской обороны. Воздушное наблюдение помогло обеспечить защиту большей части иракских 8 тыс. 278 избирательных участков от террористических нападений.

«Эти выборы принципиально отличаются от всех предыдущих выборов … что сделало их полностью или почти соответствующими международным стандартам», - отметил пресс-секретарь иракского Верховного комитета по безопасности выборов генерал-майор Галеб аль-Аттийя.

Согласно оценкам, 9 млн. иракцев из 25 млн. имеющих право голоса пришли на избирательные участки, чтобы отдать свои голоса за 3 тыс. 200 кандидатов от 167 партий, борющихся за 329 мест в парламенте.

Первоначально выборы в Ираке планировались на 2022 г., однако премьер-министр Мустафа аль-Кадхими принял решение о досрочном проведении выборов в ответ на общественные протесты с требованиями создать рабочие места и улучшить качество государственных услуг. Новый закон о выборах ускорил организацию голосования и обеспечил более широкое общественное представительство меньшинств и женщин Ирака в парламенте.

Источники: Рейтер, Би-Би-Си, Al Jazeera

Катар укрепляет военное партнерство с Турцией

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

ВМФ эмира Катара усилил свой флот церемониальным спуском на воду десантного судна, способного разместить на своей широкой палубе сотни военнослужащих.

Официально строительство десантного судна Фуваирит, имеющего возможность доставлять на берег танки, было завершено в сентябре 2021 г. на турецкой судоверфи в г. Анадолу.

Названное в честь прибрежной деревни к Катаре, судно Фуваирит может разместить на своей палубе площадью 400 квадратных метров 260 военнослужащих с полной экипировкой. Управляемое 25 моряками судно также оснащено средствами для перевозки трех танков и других боевых машин.

Это одно из шести судов, закупленных у Турции, и Катар планировал его доставку летом 2022 г.

«В течение следующих 24 месяцев мы намерены завершить все испытания и обучение и доставить их в Катар», - сказал исполнительный директор судоверфи в Анадолу Севат Рифат Атилхан о партии закупленных судов.

Помимо десантного судна Катар также заказал у судоверфи в Анадолу несколько судов, на которых будет проходить обучение курсантов Военно-морского училища Катара. В Арабском заливе страна имеет береговую линию протяженностью 563 километра.

Эти закупки происходят в рамках соглашения о совместной обороне, подписанного Катаром и Турцией в 2017 г. Для того, чтобы укрепить отношения между своими военными, две страны в 2019 г. создали турецко-катарскую объединенную тактическую группу. Ее расположенная в Дохе штаб-квартира названа в честь арабского боевого командира VII века Халида бин Аль Валида.

ВВС эмира Катара участвовали в двухнедельных многонациональных учениях «Анатолийский орел», прошедших летом 2021 г. в турецком г. Конья. Катарские пилоты отрабатывали маневры на недавно купленных у Франции истребителях Rafale из 1-й эскадрильи, базирующейся на базе ВВС в г. Тамим.

В соответствии с техническим договором, подписанным военными двух стран, Катар будет обучать пилотов в Турции в течение пяти лет и разместит там до 250 своих военнослужащих и 36 самолетов.

Источники: Naval News, Al Jazeera, ahvalnews.com

Иордания вводит в действие соглашение о безопасности с Катаром

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

В сентябре 2021 г. вступило в силу пятилетнее соглашение между Иорданией и Катаром о сотрудничестве в области безопасности, в центре внимания которого находится обмен разведывательными данными и технологиями в целях борьбы с терроризмом.

Две страны будут и дальше развивать уже существующее двустороннее сотрудничество в борьбе со всеми видами преступности: терроризмом и соответствующими финансовыми операциями; организованной преступностью; контрабандными перевозками оружия, боеприпасов, взрывчатки и ядерных, радиоактивных, химических и биологических материалов; торговлей людьми и нелегальной миграцией; контрабандой, производством и распространением наркотиков; отмыванием денег; а также подделкой паспортов, денег и других официальных документов.

В экономическом аспекте в соглашении делается упор на совместную защиту интеллектуальной собственности, технологических ресурсов, информационных систем, портов и границ. Соглашение также предполагает совместные усилия в борьбе против морского пиратства и киберпреступлений.

Министр иностранных дел Катара Мухаммед бин Абдулрахман Аль-Тани, слева, и министр иностранных дел Иордании Айман Аль Сафади на пресс-конференции в Аммане. Август 2021 г. РЕЙТЕР

Катар и Иордания поддерживают тесные дипломатические и военные отношения с тех пор, как Катар получил независимость в 1971 г. Иорданские специалисты оказали Катару помощь в экономической, образовательной и военной сфере.

Его Величество король Иордании Хуссейн бин Талал, ныне покойный, был первым мировым лидером, посетившим Катар и поздравившим Его Высочество шейха Хамада бин Калифу Аль Тани с приходом к власти в Катаре в 1995 г.

Его Величество король Иордании Абдулла II был первым арабским лидером, посетившим Доху и поздравившим Его Высочество шейха Тамима бин Хамада Аль Тани с его назначением эмиром Катара в июне 2013 г.

Военные Иордании и Катара регулярно участвуют в совместных учениях. Спецназовцы Катара принимали участие в многонациональных военных учениях «Стремительный лев» в Иордании в сентябре 2019 г., а подразделения Иордании совместно с военными из еще семи стран участвовали в учениях «Несокрушимый часовой» в Катаре в марте 2021 г.

Источники: Агентство новостей Иордании, ammonnews.net, alaraby.co.uk

Египет и Кипр укрепляют партнерство

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

Военные Египта и Кипра еще раз подтвердили свои близкие партнерские отношения, успешно проведя в сентябре военные учения «Птолемей-2021».

В ходе учений отрабатывались прицельная стрельба, ведение ближнего боя, рейд на укрытие террористов и медицинская эвакуация. Совместное участие в учениях стало тестом на боевое взаимодействие военных Египта и Кипра.

У Египта и Кипра сложились крепкие партнерские отношения в военной области. Кипрские подразделения, включая военных моряков и спецназовцев, были основными участниками двухнедельных многонациональных учений «Яркая звезда», проведенных в Египте на военной базе им. Мухаммеда Нагиба в сентябре 2021 г.

«Между военнослужащими Египта и Кипра сложились прекрасные дружеские отношения как на профессиональном, так и на личном уровне», - отметил начальник штаба Вооруженных сил Кипра генерал-полковник Демократос Зервакис на встрече со своим египетским коллегой.

Кроме того, Египет, Кипр и Греция провели трехстороннюю встречу в верхах для обсуждения партнерства и сотрудничества в вопросах, относящихся к восточному Средиземноморью, в том числе в вопросе демаркации морских границ и исключительных экономических зон.

Совсем недавно, в сентябре 2021 г., в Каире прошел президентский саммит с участием президента Египта Абделя Фаттаха ас-Сиси и президента Кипра Никоса Анастасиадеса. В повестке дня встречи были вопросы безопасности, дипломатических отношений, торговли, туризма и сельского хозяйства.

«Созданное нами стратегическое партнерство в восточном Средиземноморье требует постоянной координации действий, направленных на достижение региональной стабильности и взаимопомощи во всех вопросах, представляющих интерес для обеих стран», - подчеркнул президент ас-Сиси.

Источники: «Al Ahram», defensearabia.com, egypttoday.com

БАХРЕЙН ПЕРЕКРЫВАЕТ КАНАЛЫ ФИНАНСИРОВАНИЯ ТЕРРОРИСТОВ

СОТРУДНИКИ ЖУРНАЛА «UNIPATH»

В соответствии с разрабатываемым в Базеле «Индексом отмывания денег – 2021», в Бахрейне было зарегистрировано минимальное среди арабоговорящих стран число случаев отмывания денег.

Разрабатывающая этот индекс организация, базирующаяся в Швейцарии, свой рейтинг составляет на основе данных, предоставленных Межправительственной комиссией по финансовому мониторингу, организацией Transparency International, Всемирным банком и Всемирным экономическим форумом.

«В противостоянии отмыванию денег королевство набрало 4,5 балла и вышло на второе место после Израиля среди стран Ближнего Востока и на первое место в арабском мире», - объявил заместитель управляющего Центральным банком Бахрейна шейх Салман бин Иса Аль Калифа.

В июле 2021 г. Высший суд по уголовным делам Бахрейна осудил шесть чиновников из «Future Bank», базирующегося в Бахрейне. Каждый из них был приговорен к 10 годам тюремного заключения и штрафу в размере 2,5 млн. долл. США за участие в операциях по отмыванию денег в пользу Центрального банка Ирана.

Директор Управления финансовой разведки Министерства внутренних дел шейха Маи бинт Мухаммад Аль Калифа заявила, что ее ведомство стремится повысить региональную и мировую репутацию Бахрейна в борьбе с отмыванием денег и финансированием терроризма.

«Future Bank» был обвинен в проведении подозрительных транзакций для иранских финансовых организаций, в том числе для Центрального банка Ирана, в нарушение законов и правил Бахрейна. Общая сумма денежных переводов в различных валютах составила более 1 млрд. долл. США.

Источники: baselgovernance.org, alkhaleejonline.net.

Финансовый район в столице Бахрейна Манама

ОБМЕН ЗНАНИЯМИ

Журнал «Unipath» предоставляется бесплатно для тех, кто имеет отношение к вопросам безопасности на Ближнем Востоке, в Центральной и Южной Азии.

Сотрудничайте с журналом «Unipath»

Присылайте любые идеи для репортажей, письма редактору, статьи-мнения, фотографии и другие материалы в редколлегию журнала «Unipath» на адрес CENTCOM.UNIPATH@MAIL.MIL

Советы о присылаемом материале

- Предпочтительно, чтобы материал подавался на вашем родном языке. «Unipath» обеспечит перевод.
- Статьи не должны превышать 1,5 тыс. слов.
- Просьба включать краткую биографию и контактную информацию с каждым подаваемым материалом.
- Размер фотофайлов должен быть не менее 1 Мбайт.

Права

Авторы сохраняют все права на свой первоначальный материал. Однако, мы оставляем за собой право редактировать статьи в отношении размера и стиля. Представление статьи не гарантирует ее опубликование. Присылая материал в журнал «Unipath», вы соглашаетесь на эти условия.

Для **БЕСПЛАТНОЙ** подписки свяжитесь с нами по электронной почте: CENTCOM.UNIPATH@MAIL.MIL

или пишите по адресу:
Unipath
U.S. Central Command
7115 S. Boundary Blvd.
MacDill AFB, FL 33621 USA

Просим вас указывать имя и фамилию, род занятий, должность или звание, почтовый адрес и адрес электронной почты.

HTTPS://UNIPATH-MAGAZINE.COM/RU