ТОМ 7, НОМЕР 2, 2016

per Concordiam

Журнал по проблемам безопасности и обороны Европы

■ **БАЛТИЙСКАЯ КИБЕРОБОРОНА**
Страны подписывают важное соглашение

■ **КИБЕРТЕРРОРИЗМ**
Классификация атак по степени опасности

■ **ЗАЩИТА УКРАИНЫ**
Киев стоит перед лицом целого ряда угроз

■ **БОРЬБА С «БОКО ХАРАМ»**
Война Нигерии в сети против терроризма

ПЛЮС
Партнерство ради мира
Казахстан в поисках безопасности
Подход Грузии к киберсфере

ОБМЕН ИНФОРМАЦИЕЙ

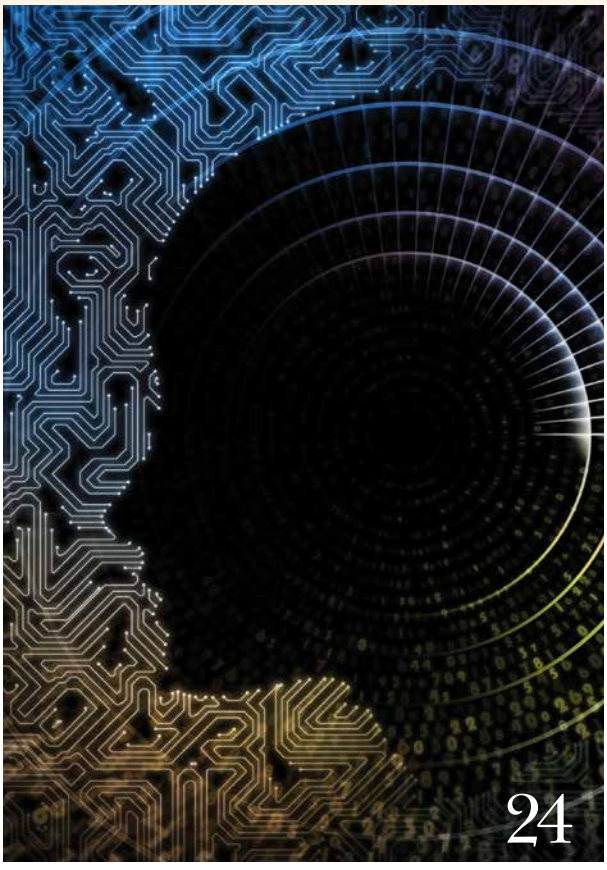
Совместный подход к кибербезопасности

Содержание

основные статьи

НА ОБЛОЖКЕ

Для кибератак практически никогда не существует национальных границ. Поэтому стратегии, направленные на предотвращение и отражение таких атак, а также на реагирование на них, должны быть ориентированы на региональный и глобальный подход. GETTY IMAGES



В каждом номере

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Добро пожаловать на страницы двадцать шестого номера журнала *per Concordiam*. Кибербезопасность является одним из важнейших вызовов, стоящих перед нами сегодня. Киберпространство, взаимосвязанное и взаимозависимое на глобальном уровне, лежит в основе современного общества и играет критически важную роль в мировой экономике, гражданской инфраструктуре, общественном порядке и национальной безопасности. Информационные технологии преобразовали глобальную экономику, соединив людей и рынки по всему миру. Для полной реализации потенциала цифровой революции пользователям необходимо быть уверенными в том, что их чувствительная информация находится в безопасности, а функционирование торговли и инфраструктуры не нарушено. Государствам же необходимы надежные и жизнестойкие сети, способные обеспечить поддержку национальной безопасности и процветания.

Страны нуждаются в разработке и реализации национальных стратегий кибербезопасности для защиты своей критической киберинфраструктуры и снижения киберугроз. Для защиты киберпространства требуется четкое видение и умелое руководство, а также способность справляться с постоянными переменами в приоритетах, политиках, технологиях, образовании, законах и международных соглашениях. Подлинная приверженность кибербезопасности должна быть продемонстрирована на самых высоких уровнях власти, бизнеса и гражданского общества, и лишь тогда страны смогут осуществлять инновации и применять самые передовые технологии, одновременно обеспечивая защиту национальной безопасности, глобальной экономики и права человека на свободное выражение своего мнения. Так, например, в процессе защиты своих систем связи и информации НАТО реагирует на миллионы постоянно эволюционирующих киберугроз, параллельно укрепляя отношения по взаимному обмену информацией с промышленностью и научным сообществом.

Обмен информацией играет жизненно важную роль в кибербезопасности. Он обеспечивает передачу информации между правительственным и частным секторами, а также между субъектами частного сектора. Обмен информацией может помочь быстрее выявить киберугрозу и организовать меры реагирования на нее. Для облегчения обмена информацией между заинтересованными представителями государственного и частного секторов могут быть организованы центры обмена информацией по сетевой безопасности.

Резидентский курс «Программа по изучению вопросов кибербезопасности (ПВКБ)» Центра им. Маршалла включает в себя доклады и обсуждения стратегических и политических решений, способствующих достижению кибербезопасности. В курс также входят учебные модули по разработке стратегии кибербезопасности, управлению киберпространством, частно-государственным партнерствам, общегосударственным решениям и важности защиты критической инфраструктуры. Существует огромная потребность в образовании и подготовке, которые акцентированы на киберсфере, и я призываю вас занять активную позицию путем повышения кибербезопасности в рамках вашей организации. Для решения сложных стратегических, политических и технических проблем в киберсфере потребуются новаторские действия со стороны руководителей всех организаций.

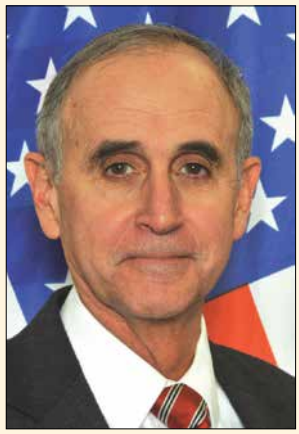
В данном номере журнала *per Concordiam* содержатся предложения по решению наиболее сложных проблем кибербезопасности, таких как:

- наращивание усилий в области национальной кибербезопасности на всех уровнях общества;
- повышение безопасности и жизнестойкости критической инфраструктуры;
- укрепление частно-государственных партнерств;
- расширение индивидуальных возможностей и защита права на неприкосновенность частной жизни;
- сдерживание, предотвращение и препятствование злонамеренной деятельности в киберпространстве;
- улучшение реагирования на киберинциденты.

Мы приветствуем ваши комментарии и мнения по этой теме. Ваши ответы могут быть опубликованы в следующем выпуске журнала, который будет посвящен борьбе с транснациональными преступными организациями. Пожалуйста, пишите нам по адресу editor@perconcordiam.org

Искренне ваш,

Кит В. Дейтон
Директор



Кит В. Дейтон
Директор
Центр им. Маршалла

Кит Дейтон вышел в отставку с военной службы в Сухопутных войсках США в конце 2010 г. в звании генерал-лейтенанта, прослужив в вооруженных силах более 40 лет. Его последним назначением на действительной военной службе была должность Координатора США по вопросам безопасности между Израилем и Палестиной в Иерусалиме. В его послужном списке служба в качестве офицера-артиллериста, а также работа на посту офицера по военно-политическим вопросам при штабе Сухопутных войск США в Вашингтоне (округ Колумбия) и военного атташе США в Российской Федерации. В его послужном списке работа на посту директора аналитической группы по Ираку в ходе операция «Свобода Ирака». Генерал-лейтенант Дейтон проходил стажировку в Колледже для старшего руководящего состава при Гарвардском университете. Он также являлся старшим стипендиатом от Сухопутных сил США в Совете по международным отношениям в Нью-Йорке. Генерал-лейтенант Дейтон имеет степень бакалавра истории от Колледжа Вильгельма и Марии, степень магистра истории от Кембриджского университета, а также степень магистра международных отношений от Южнокалифорнийского университета.

Дэниэл П. Багге является руководителем Отдела стратегии и политики в Национальном центре кибербезопасности Управления национальной безопасности Чешской Республики. Имеет степень магистра в области исследований по международной безопасности, полученную по окончании аспирантской программы, которая проводится совместно Центром им. Маршалла и Университетом Бундесвера в Мюнхене.

Андрия Гоциридзе является директором Бюро кибербезопасности Министерства обороны Грузии. Эксперт в области реформирования сектора безопасности, противодействия коррупции и внешней разведки. Под его руководством Бюро кибербезопасности разработало первую в Грузии политику и стратегию обороны в сфере кибербезопасности и инициировало актуальные проекты в области кибербезопасности.

Анна Гусарова является старшим научным сотрудником Казахстанского института стратегических исследований. Преподает курсы по дипломатии и международному терроризму в Казахстанско-немецком университете в Алматы. Имеет степени бакалавра американистики и магистра в области исследований по вопросам безопасности Центральной Азии от указанного университета.

Альваро Хосе Чавес Гузман является директором Департамента общественной безопасности и инфраструктуры Министерства национальной обороны Колумбии. Ранее исполнял обязанности советника Заместителя министра обороны по вопросам политики и международных отношений, а также секретаря Заместителя министра обороны по вопросам стратегии и планирования. Имеет степени бакалавра политологии и магистра международных отношений и переговоров от Университета Анд.

Аарон Хьюз являетсяЗаместителем помощника министра обороны США по киберполитике. Специализируется на инновационных технологиях для разведывательного сообщества. Имеет степени бакалавра от Университета Вирджинии, магистра по телекоммуникациям и компьютерным наукам от Университета Джорджа Вашингтона и магистра делового администрирования от Стэнфордской высшей школы бизнеса.

Наталья Спину является руководителем Центра кибербезопасности Республики Молдова. Занимала должности начальника отдела Центра специальных телекоммуникаций Молдовы и координатора проектов в Центре информации и документации о НАТО. Прошла подготовку в рамках Программы углубленного изучения проблем безопасности в Центре им. Маршалла в 2012 г. и имеет степень магистра от Европейского института Университета Женевы.

Мартина Улманова является специалистом по политике в области кибербезопасности в Национальном центре кибербезопасности Чешской Республики. Ее опыт работы связан со сферой учений в области кибербезопасности. Помимо этого, она читает лекции в университетах на тему кибербезопасности. Имеет степень магистра исследований в области стратегии и безопасности от Университета им. Масарика в Брно.

per Concordiam

Журнал по проблемам безопасности и обороны Европы

ЗАЩИТА КИБЕРПРОСТРАНСТВА

Том 7, Номер 2, 2016

Европейского центра по изучению вопросов безопасности им. Дж. К. Маршалла:

Центр имени Маршалла

Европейский Центр по исследованию вопросов безопасности имени Джорджа К. Маршалла – это совместный немецко-американский центр, основанный в 1993 г. Задачей центра является поддержка диалога и понимания между европейскими, евразийскими, североамериканскими и другими государствами. Тематика его очных курсов обучения и информационно-разъяснительных мероприятий: большинство проблем безопасности в 21 веке требуют международного, межведомственного и междисциплинарного подхода и сотрудничества.

Контактная информация:

per Concordiam editors
Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

per Concordiam – профессиональный журнал, ежеквартально публикуемый Европейским центром исследований по вопросам безопасности имени Джорджа К. Маршалла и посвященный вопросам обороны и безопасности Европы и Евразии, предназначенный для ученых и специалистов, занимающихся проблемами обороны и безопасности. Мнения, выражаемые в этом журнале, не всегда представляют политику или точку зрения этого учреждения, равно как и любых других государственных органов Германии или США. Все статьи, кроме тех, где указаны авторы, написаны сотрудниками редакции *per Concordiam*. Мнения, выражаемые в статьях, написанных авторами, не являющимися сотрудниками редакции, представляют исключительно точку зрения конкретного автора. Министр обороны принял решение, что публикация этого журнала необходима в целях работы с общественностью в соответствии с требованиями законодательства, распространяющегося на Министерство обороны США.

ISSN 2166-4080 (печатные издания)
ISSN 2166-417X (интернет)

per Concordiam теперь в ИНТЕРНЕТЕ

Благодаря цифровой версии журнала вы всегда будете в курсе последних событий, связанных со всеобщей безопасностью в Европе и Евразии

http://perconcordiam.com

Отправляйте статьи, отзывы и запросы на подписку в Центр им. Маршалла по адресу: editor@perconcordiam.org

ДОСТИЖЕНИЕ СДЕРЖИВАНИЯ В КИБЕРПРОСТРАНСТВЕ

Новая стратегия Министерства обороны США ориентируется на предотвращение

Эрон Хьюз, Заместитель помощника министра обороны по киберполитике

Враждебные игроки в киберпространстве представляют собой комплексный и динамичный набор угроз, ответы на которые принимающим решения лицам придется искать в XXI веке. Киберугрозы интересам Соединенных Штатов характеризуются возрастающей серьезностью и сложностью и исходят как от государственных, так и от негосударственных игроков.

Как и государства, которые обладают передовыми киберпотенциалами и стратегиями – от незаметного проникновения в компьютерные сети до кражи интеллектуальной собственности – преступные и террористические сети тоже расширяют свои киберпотенциалы и кибероперации. Низкая стоимость и глобальная распространенность вредоносного программного обеспечения снизили барьеры для входа в данную область и облегчили осуществление менее крупными игроками атак в киберпространстве. В мире также происходит слияние угроз, исходящих от государственных и негосударственных игроков, что может не только подорвать стабильность, но и усложнить потенциальные ответные меры со стороны Министерства обороны (МО) США и иных органов.

За последние годы имело место несколько резонансных злонамеренных нападений, произошедших в киберпространстве или с его помощью, которые привлекли внимание общественности, в том числе инциденты, жертвами которых стали кинокомпания «Sony Pictures Entertainment», Управление кадровой службы США, несекретная сеть Объединенного комитета начальников штабов МО США, сеть французского телеканала «TV5 Monde» и энергосистема Украины. Ввиду продолжающихся резонансных инцидентов такого рода вполне естественно, что профессионалы в области национальной безопасности и исследователи в области международных отношений задаются вопросом, можно ли что-либо сделать для воспрепятствования злонамеренной деятельности в киберпространстве.

Это важный вопрос, и в настоящее время МО ищет на него ответ, так как практически в любой нашей деятельности мы в значительной степени полагаемся на киберпространство. У МО в киберпространстве есть три задачи. Первая состоит в защите наших собственных сетей, систем и информации. Вторая состоит в защите США и их интересов от серьезных кибератак. Нашей третьей задачей является обеспечение интегрированных киберпотенциалов, в том числе вариантов наступательных кибердействий, которые могли бы, по приказу президента, дополнить иные военные потенциалы нашей страны.

Культивирование кибersдерживания

Перед лицом растущей киберугрозы и необходимости выполнения наших задач в киберпространстве МО разрабатывает и реализует комплексную стратегию сдерживания кибератак против самого Министерства и американских интересов. Одна из трудностей

Адмирал Майкл Роджерс, возглавляющий Кибернетическое командование США, директор Агентства национальной безопасности и руководитель Центральной службы безопасности, возглавляет усилия США по противодействию киберугрозам XXI века. AFP/GETTY IMAGES

состоит в том, чтобы сделать стратегию достаточно широкой для того, чтобы она затрагивала всех разнообразных и многочисленных злоумышленников в киберпространстве. Стратегия также должна принимать во внимание типы кибератак, которые мы пытаемся предотвратить. Учитывая масштаб киберпространства и широкую доступность вредоносного программного обеспечения, МО должно смотреть фактам в лицо и признать, что сдержать все кибератаки невозможно. Продолжая развивать свое подразделение по выполнению миссий в киберпространстве и свои киберпотенциалы в целом перед лицом растущих угроз, МО полагает, что наилучшим путем достижения сдерживания кибератак на американские интересы является использование всей совокупности действий и потенциалов США, что включает в себя ключевые элементы и инструменты, такие как декларируемая политика США, укрепление потенциалов индикации и оповещения, оборонительная тактика, эффективные процедуры реагирования, а также общая жизнестойкость сетей и систем страны. Сдерживание государственных и негосударственных группировок в киберпространстве требует общегосударственного подхода, и МО будет выполнять свою роль в качестве одного из инструментов государственной власти, находящихся в распоряжении президента.

Механизм сдерживания заключается в убеждении потенциального противника в том, что в ответ на нападение он заплатит неприемлемую цену (навязывание цены), и в уменьшении вероятности того, что какое-либо нападение будет успешным (воспрещение достижения цели). Таким образом, США должны обладать способностью декларировать и демонстрировать эффективные потенциалы реагирования, чтобы сдержать осуществление кибернападения противником; разрабатывать эффективные оборонительные потенциалы, чтобы предотвратить успех возможного кибернападения; и повысить общую жизнестойкость американских систем на случай, если кибернападение преодолеет нашу оборону. В качестве составляющей эффективной тактики сдерживания США нуждается в значительных разведывательных возможностях, киберкриминалистике и потенциалах индикации и оповещения для снижения уровня анонимности в киберпространстве и повышения надежности установления авторства атак. Рассмотрим указанные четыре элемента, играющие основополагающую роль в культивировании сдерживания, более детально.

Министр обороны США Эштон Картер выступает в Конгрессе США в феврале 2016 г. Картер продвигал создание в структуре вооруженных сил США кибернетического командования с целью укрепления киберпотенциалов. АССОШИЭЙТЕД ПРЕСС

Реагирование: с помощью различных документов, докладов и официальных заявлений президента и министра обороны США озвучили свою готовность ответить на кибератаку на американские интересы. В случае такой атаки ее результаты оцениваются на индивидуальной и фактологической основе президентом и его командой по национальной безопасности. Серьезные последствия подобной атаки могут включать в себя человеческие жертвы, материальный ущерб, а также значительные негативные последствия в области внешней политики и экономики. В случае принятия президентом решения о применении ответных мер на кибератаку на американские интересы США оставляют за собой право принять указанные меры тогда, там и так, как посчитают нужным, с использованием подходящих инструментов силы США. Нашим противникам следует знать, что предпочтение, отдаваемое нами сдерживанию, и наша оборонительная тактика не уменьшают нашу готовность использовать в случае необходимости военные меры, в том числе киберпотенциалы. И когда мы перейдем к действиям – защитным или иным, обычными средствами или в киберпространстве – МО будет действовать в соответствии с требованиями международного и американского законодательства.

Воспрещение: МО работает над развитием своих оборонительных потенциалов с целью защиты своих сетей и защиты страны от нападений с использованием новейших киберсредств. Параллельно с этим мы ведем работу с другими министерствами и органами власти, нашими международными союзниками и партнерами, а также с частным сектором для укрепления сдерживания через воспрещение путем повышения кибербезопасности.

Когда министр обороны США Эштон Картер представлял киберстратегию МО в 2015 г., он привел пример недавнего злонамеренного киберинцидента, в котором сенсоры, охраняющие несекретные сети

МО, обнаружили российских хакеров, проникших в одну из наших сетей через старую и неисправленную уязвимость. Хотя тот факт, что злоумышленникам удалось получить некоторый доступ к нашим несекретным сетям, вызывает озабоченность, мы тем не менее смогли быстро обнаружить проникновение, а команда реагирования на инциденты выслеживала злоумышленников уже менее чем через 24 часа после того, как оно произошло. Получив ценную информацию об их тактике и проанализировав их сетевую активность, мы выгнали их из нашей сети способом, минимизирующим шансы этих хакеров на повторное проникновение. У этой истории счастливый конец, но это не единственная причина, по которой министр Картер решил ее рассказать: открытое обсуждение нашей способности быстро обнаружить атаку, установить ее авторство и выдворить злоумышленника из наших военных сетей также имеет и важный сдерживающий эффект.

Кибернетическое командование США, Агентство национальной безопасности и Центральная служба безопасности возглавляют усилия США по обороне и реагированию в киберсфере. AFP/GETTY IMAGES

Жизнестойкость: так как мы не можем гарантировать воспрещение всех кибератак, МО работает над созданием жизнестойких систем с избыточностью, способных обеспечить продолжение нашей жизненно важной деятельности в условиях кибератак, имеющих нарушающий или разрушающий эффект. Важным компонентом указанного «обеспечения выполнения миссии» является идентификация и защита сетей и систем, имеющих наиболее критическое значение для деятельности МО.

В более широком смысле другим органам власти также следует работать с владельцами и операторами критической инфраструктуры, а также с частным сектором для разработки жизнестойких систем с избыточностью, способных выдержать атаки. Подобные меры могут помочь убедить потенциальных противников в жизнестойкости американских сетей и систем и, следовательно, в тщетности попыток кибернападения.

Установление авторства: представление о том, что в киберпространстве процветает анонимность, способствует злонамеренной киберактивности со стороны государственных и негосударственных группировок. Следовательно, укрепление потенциалов по установлению авторства является основополагающим элементом эффективной стратегии киберсдерживания. МО и разведывательное сообщество США осуществили значительные вложения в разработку потенциалов по сбору, анализу и распространению данных от всех источников, которые служат для снижения степени анонимности действий в киберпространстве. Установление авторства позволяет МО, а также другим министерствам и органам власти проводить операции по реагированию на кибератаки и их воспрещению с большей степенью уверенности.

Установление авторства – как публичное, так и при закрытых дверях – может сыграть важную роль в том, чтобы заставить киберигроков отказаться от проведения атак. МО будет продолжать тесное сотрудничество с частным сектором и другими министерствами и органами правительства США в области укрепления потенциалов по установлению авторства. Эта работа станет еще более важной частью сдерживания по мере освоения более продвинутых киберпотенциалов группами активистов, преступными организациями и иными игроками.

Заключение

Многие специалисты и ученые ссылаются на роль сдерживания в предотвращении ядерного конфликта в годы Холодной войны. И хотя ими зачастую проводятся параллели с успехом стратегии сдерживания во время Холодной войны, мы должны помнить, что сдерживание в сегодняшнем киберпространстве носит намного более сложный характер. Ввиду высокой стоимости и сложности ядерного оружия существовало лишь несколько игроков, которых нужно было сдерживать, и все они являлись государствами. Ситуация в сегодняшнем киберпространстве совершенно иная: в интернете можно легко и за небольшую плату найти даже самое продвинутое вредоносное программное обеспечение. По мере того как мы пытаемся применить уроки Холодной войны к современной угрозе кибератак, следует помнить о том, что само понятие и практика сдерживания в ядерном веке не возникли одномоментно в готовом виде, а развивались с течением времени. Схожим образом МО будет продолжать культивировать сдерживание, вкладывая усилия в развитие своего подразделения по выполнению миссий в киберпространстве и соответствующих потенциалов. Реагирование, воспрещение, жизнестойкость и установление авторства являются фундаментом, на котором основывается наша оборонительная тактика. □

ISTOCK

Определение понятия «КИТЕ

БЕРРОРИЗМ»

БОЛЬШИНСТВО ЭКСПЕРТОВ НЕ МОГУТ ДОГОВОРИТЬСЯ ОБ ОПРЕДЕЛЕНИИ, УСТРАИВАЮЩЕМ ВСЕХ

Рубен Тейтель

Ученые, практикующие юристы и международные организации испытывают трудности с определением понятия «кибертерроризм». Кроме того, существует путаница в отношении разницы между понятиями «киберпреступление» и «кибертерроризм». Хотя данная статья посвящена понятию кибертерроризма, я кратко остановлюсь и на понятии киберпреступления, чтобы подчеркнуть различия между ними. Существующие определения кибертерроризма оставляют возможность для споров, поэтому я предлагаю свое определение: кибертерроризм – это использование киберпространства негосударственным субъектом в целях нарушения функционирования компьютерных систем, распространения чувства страха или приносящее физический ущерб и, косвенным образом, вред здоровью, либо вызывающее такие перебои в их работе, которые серьезно угрожают репутации жертвы, производимое в политических, идеологических или религиозных целях.

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «КИБЕРАТАКА»

Возможные напоминающие кибератаку сценарии включают в себя вирус, шифрующий финансовые документы или выводящий из строя фондовый рынок, ложное сообщение, приводящее к остановке атомного реактора или перебою в работе авиадиспетчерской службы, приводящему к авиакатастрофам. Определение понятия кибератаки необходимо для того, чтобы отличать ее от кибертерроризма. Существует множество определений понятия «кибератака», и ниже приведены некоторые из них.

Управление ООН по наркотикам и преступности определяет кибератаку следующим образом:

> «Под понятием “кибертерроризм” обычно понимают преднамеренную эксплуатацию компьютерных сетей с целью предпринять атаку. Такие атаки, как правило, предпринимаются для нарушения надлежащего функционирования целей, таких как компьютерные системы, серверы или лежащая в их основе инфраструктура, при помощи хакинга, технологий APT (развитая устойчивая угроза), компьютерных вирусов, вредоносного программного обеспечения, заливки и иных средств несанкционированного или злонамеренного доступа».[1]

В Единой доктрине информационных операций Объединенного комитета начальников штабов ВС США кибератаки определены как:

> «преднамеренные действия по изменению или нарушению функционирования компьютерных систем или хранящейся в них информации, а также их обману, ослаблению или уничтожению».

Оксфордский словарь определяет кибератаку как:

> «попытку хакеров повредить или уничтожить компьютерную сеть или систему».

Мауно Пиэльгас – исследователь, работающий в Центре передового опыта НАТО в области коллективной кибероборонь в Эстонии, – дает следующее определение кибератаки в главе, написанной им для книги «Режим мирного времени для деятельности государств в киберпространстве»:

> «под термином “атака” понимается любая попытка уничтожить, раскрыть, изменить, вывести из строя, украсть, получить несанкционированный доступ или несанкционированным образом использовать что-либо, что представляет ценность для организации».

Дать определение понятия «кибертерроризм» сложнее. Существует множество аспектов, затрудняющих принятие решения о том, может ли кибератака быть названа актом кибертерроризма. Однако прежде чем переходить к обсуждению данного вопроса, важно понять характеристики терроризма.

Следующие характеристики терроризма, изложенные Брусом Хоффманом в книге «Терроризм – взгляд изнутри», являются общепринятыми. Стремясь отличить террористов от прочих типов преступников и бойцов нерегулярных сил, а терроризм от иных форм преступности и нерегулярной войны, мы приходим к пониманию того, что терроризм является:

- исключительно политическим в своих целях и мотивах.
- насильственным или, что не менее важно, угрожающим насилием.
- предназначенным для оказания длительного психологического воздействия, а не только уничтожения конкретной жертвы или объекта.
- проводимым организацией с распознаваемой системой управления или конспиративной ячеечной структурой (чьи представители не носят униформу или знаки отличия) либо лицами или небольшой группой лиц, находящихся под непосредственным влиянием или вдохновленных идеологическими целями или примером существующего террористического движения и/или его лидеров; и, наконец, совершаемым внутринациональной группировкой или негосударственным субъектом.

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «КИБЕРТЕРРОРИЗМ»

Установление авторства

Для того чтобы кибератака рассматривалась как акт кибертерроризма, она должна быть совершена террористической группировкой. Это вопрос установления авторства, а установление авторства кибератаки является сложной задачей. В отличие от реального мира киберпространство не признает национальных границ. Интернет-пользователь в стране А может купить продукт в стране Б, даже не осознавая, что он покупает продукт в другой стране. Кроме того, интернет-пользователь может работать с различных IP-адресов, используя прокси-серверы для сокрытия своей онлайн-идентичности или же использовать анонимный интернет-браузер, такой как «Tor», и так называемую Глубокую паутину, или Теневой Интернет, о чем подробно говорится в докладе, опубликованном в 2001 г. в журнале «The Journal of Electronic Publishing». В статье, опубликованной в 2012 г. в газете «The Telegraph», говорится, что педофилы пользуются последними двумя средствами для обмена порнографическими фото- и видеоматериалами, и затрудняет их выявление и установление их местонахождения правоохранительными органами.

В ОТЛИЧИЕ ОТ РЕАЛЬНОГО МИРА КИБЕРПРОСТРАНСТВО НЕ ПРИЗНАЕТ НАЦИОНАЛЬНЫХ ГРАНИЦ.

Другой метод сокрытия своей идентичности в интернете состоит в использовании виртуальных частных сетей (VPN). Пиэльгас пишет, что виртуальные частные сети часто применяются для подключения к сети компании извне ее офиса, что позволяет сотрудникам работать с внутренними документами компании, не взаимодействуя напрямую с интернетом и, следовательно, с потенциальными злонамеренными пользователями. Настроить VPN достаточно просто, и этим могут злоупотреблять злонамеренные игроки, так как в результате их трафик будет зашифрован. «Обратное прослеживание», также известное как «трассировка в обратном направлении», состоит в использовании технического процесса с применением инструмента «traceroute» для установления IP-адреса нападающего. Правоохранительные органы используют данный процесс, чтобы определить, является ли атака результатом деятельности группы хакеров или одного человека.

Однако такой вещи, как полная анонимность в интернете, не существует. В теории обратное прослеживание должно всегда приводить к преступнику. Но правоохранительные органы могут ошибиться в установлении авторства, то есть несправедливо обвинить того, кто не имел отношения к проведению данной кибератаки. Это усложняет обратное прослеживание для правоохранительных органов. Пиэльгас поясняет:

> «С развитием различных технологий обеспечения анонимности трудность установления авторства становится одним из основных вызовов в деле уменьшения общей незащищенности, исходящей из киберпространства, и отслеживания конкретных злонамеренных игроков. Правильное установление авторства необходимо для реагирования на киберинциденты как в оперативном, так и в правовом смысле. Ошибочное установление авторства является проблемой противоположного характера, в которой атаку пытаются представить исходящей из другого источника (обвиняя кого-то другого). Вдобавок к замедлению процесса установления авторства это может привести к рискованным ситуациям, в которых вина возлагается на невиновное лицо, организацию или страну. Последствия могут варьироваться от конфликтов и недоверия между сторонами до придания неловким инцидентам широкой известности».

Насилие в киберпространстве

Одной из характеристик терроризма является насилие или его угроза. Всемирная организация здравоохранения определяет насилие как «Преднамеренное применение физической силы или власти, действительное или в виде угрозы, направленное против себя, против иного лица, группы лиц или сообщества, результатом которого являются (либо имеется высокая степень вероятности таковых) телесные повреждения, смерть, психологическая травма, отклонения в развитии или различного рода ущерб». Однако киберпространство – это виртуальный мир, пространство компьютеров, серверов, модемов и интернета, так что вопрос о том, может ли в нем происходить какое-либо насилие, является спорным. Хотя вирус «Stuxnet» оказался способным повредить центрифуги на ядерном заводе в Иране, эти повреждения не были нанесены при помощи прямой физической силы. Кибератака оказала воздействие на компьютерную систему, что привело к физическому ущербу. К примеру, автомобильная бомба наносит непосредственный физический ущерб, в то время как вирусу Stuxnet потребовался дополнительный шаг для

нанесения физического урона. Но как же быть с насилием в киберпространстве: цифровыми нападениями, совершаемыми из одного киберэлемента и имеющими цель нарушить функционирование другого кибер-, или виртуального, элемента? Для устранения расхождения между физическим и виртуальным мирами в плане насилия необходимо различать физическое насилие и кибернасилие. Также могут потребоваться определения таких понятий, как «физическая кибератака» и «виртуальная кибератака» или «физический кибертерроризм» и «виртуальный кибертерроризм».

Кибертерроризм и киберпреступность

Проведение различий между преступными и террористическими актами в киберпространстве, а также иными видами злонамеренной деятельности является сложной задачей. Четкое разграничение различных форм злонамеренной кибердеятельности играет важную роль в расследовании и уголовном преследовании этих преступлений.

Согласно опубликованному в 2013 г. докладу Исследовательской службы Конгресса США под названием «Киберпреступность. Концептуальные вопросы для Конгресса и правоохранительных органов США», киберпреступления воспринимаются как цифровые версии традиционных преступлений. Например, личные данные могут быть украдены в результате взлома база данных клиентов интернет-магазинов, в то время как традиционный преступник должен физически украсть кошелек с документами. Другие примеры киберпреступлений включают в себя мошенничество с использованием банковских карт, взлом компьютерных систем компании и распространение и/или просмотр детской порнографии. Далее, деятельность киберпреступников отличается от деятельности кибертеррористов тем, что они преследуют различные цели и имеют различную мотивацию. В опубликованном в 2010 г. докладе говорится, что киберпреступники мотивированы прибылью и занимаются такими преступлениями, как кража денег или информации, которую можно продать.

Террористы же – и, следовательно, кибертеррористы – мотивированы идеологией, как говорится в статье Международного центра исследования политического насилия и терроризма, или политическими убеждениями, связанными с преступлениями, наносящими больший ущерб обществу и создающими атмосферу страха и опасений. Однако в то же время кажется, что происходит слияние преступности и терроризма. Основой террористических операций являются деньги. Без них практически невозможно приобрести материалы, необходимые для осуществления атаки. Для финансирования своей деятельности

ПРОВЕДЕНИЕ РАЗЛИЧИЙ МЕЖДУ ПРЕСТУПНЫМИ И ТЕРРОРИСТИЧЕСКИМИ АКТАМИ В КИБЕРПРОСТРАНСТВЕ, А ТАКЖЕ ИНЫМИ ВИДАМИ ЗЛОНАМЕРЕННОЙ ДЕЯТЕЛЬНОСТИ ЯВЛЯЕТСЯ СЛОЖНОЙ ЗАДАЧЕЙ.

террористы прибегают к преступлениям, таким как незаконный оборот наркотиков, но также пользуются и цифровыми источниками. Однако эта конвергенция все больше усложняет задачу классификации человека как преступника или террориста.

Различие между киберпреступностью и кибертерроризмом достаточно ясно; однако правоохранительным органам сложно установить личность и мотивацию преступника, совершившего атаку в киберпространстве, и таким образом определить, была ли данная атака преступлением или актом терроризма.

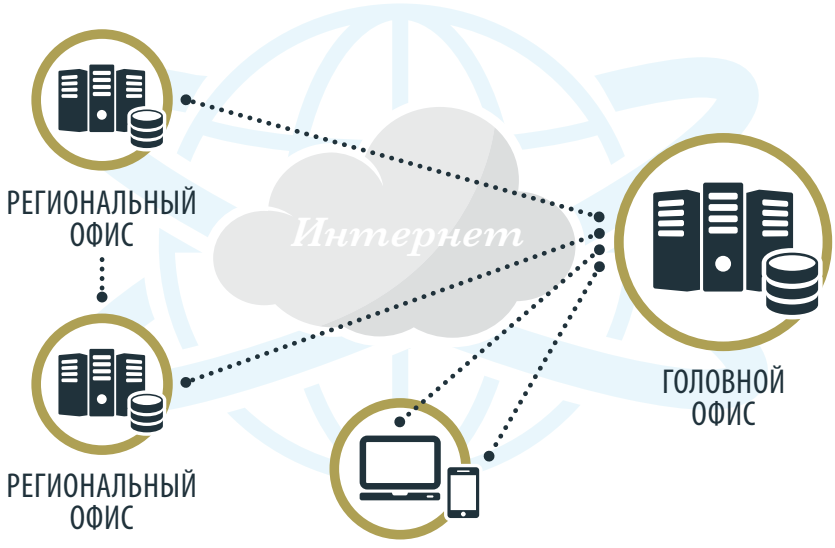
Террористы ищут внимания

Менее сложным, но все равно заслуживающим упоминания вопросом является то, что террористы и иные негосударственные субъекты зачастую ищут внимания общественности. Террористы хотят, чтобы власти знали, что именно они несут ответственность за взрыв бомбы или авиакатастрофу и что они совершили этот акт по идеологическим или политическим причинам. Газета «The Daily Mail» пишет, что террористы информируют общественность, размещая видео на YouTube или посылая твит со своего аккаунта в Твиттере, Однако на сегодня нет свидетельств того, что террористическая группировка, такая как «Аль-Каида», совершила кибератаку, приведшую к значительному ущербу. Возможно, у террористов пока нет знаний и опыта для проведения атаки на особо важную цель, или же они считают киберпространство недостаточно публичной сферой. В то время как кибератаки могут нарушить функционирование критической инфраструктуры, такой как банки, автомобильная бомба, вероятно, нанесет больше ущерба и может даже оказаться дешевле. Кроме того, автомобильная бомба оказывает большее влияние на общество и оказывает более сильное психологическое воздействие. Поэтому привлекательность киберпространства для террористов вызывает сомнения. Однако существует несколько

БАНКИ *являются* ПОПУЛЯРНЫМИ ЦЕЛЯМИ

Банки являются популярными целями среди хакеров. Распространенными видами кибератак на банки являются распределенная атака «отказ в обслуживании» (DDoS) и целевой фишинг. Целью обоих видов атак является получение информации от клиентов, которая затем используется для получения дальнейшей информации при помощи звонка в службу технической поддержки банка. В конце концов хакеры запрашивают денежные переводы. Хакеры выбирают время проведения DDoS-атак таким образом, чтобы те служили отвлекающим маневром, дающим им возможность использовать перегруженность сотрудников службы технической поддержки. Хотя эти действия не достигают уровня кибертерроризма, банки являются критически важной частью любого общества. Если их деятельность будет нарушена, многие компании не смогут продолжать свою повседневную деятельность, что нанесет ущерб экономике.

ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ (VPN)



Соединение через VPN является зашифрованным и защищено от публичного интернета.

ИЛЛЮСТРАЦИЯ PER CONCORDIAM

Источник: http://www.bankinfosecurity.com/banking-cyber-attack-trends-to-watch-a-6482/op-1

сценариев, в которых кибератака может быть классифицирована как кибертерроризм, например, атака на энергетическую систему страны.

ВОЗМОЖНЫЙ КИБЕРТЕРРОРИЗМ?

Критическая инфраструктура и системы управления производственными процессами являются привлекательными целями. Прекращение или нарушение их деятельности может привести к человеческим жертвам и оказать значительное психологическое воздействие. Марк Эльсберг описывает один из наихудших вариантов развития событий в своей книге «Blackout», вышедшей в 2012 г.:

> «Хакеры-кибертеррористы получили доступ к системам управления ООО “TenneT”, национального оператора системы электропередачи Нидерландов, отвечающего за поставку электроэнергии в Нидерланды и часть Германии. Несколько часов спустя хакеры отключили электросеть при помощи распределенной атаки “отказ в обслуживании”, что вызвало отключение электричества во всей стране. Больницы, все более полагающиеся на электронные системы в деле ухода за пациентами, не могут нужным образом лечить своих пациентов, что приводит к большому количеству смертей. До аварийно-спасательных служб нельзя дозвониться, а линии связи не работают. Граждане не имеют представления о том, что происходит, и хотя в первые часы отключение электроэнергии показалось незначительной проблемой, сейчас люди начинают паниковать. Власти ведут расследование, если это вообще возможно, и

оказывают помощь лишь людям, нуждающимся в неотложной медицинской помощи. Водоочистные сооружения не работают, что приводит к плохому качеству питьевой воды. Работа пищевой промышленности нарушена, что в конце концов приводит к нехватке продовольствия. Весьма вероятно, что люди скоро начнут мародерствовать, чтобы выжить».

СУЩЕСТВУЮЩИЕ ОПРЕДЕЛЕНИЯ ПОНЯТИЯ «КИБЕРТЕРРОРИЗМ»

В 2000 г. эксперт по информационной безопасности Дороти Е. Деннинг, выступая перед Специальной комиссией по вопросам терроризма Палаты представителей Конгресса США, предложила следующее определение понятия «кибертерроризм»:

> «… конвергенция терроризма и киберпространств. Обычно означает незаконные атаки или угрозы проведения атаки, направленные против компьютеров, сетей и хранящейся в них информации с целью запугивания или принуждения правительства или населения страны для достижения политических или социальных целей. Более того, чтобы быть квалифицированной в качестве акта кибертерроризма, атака должна привести к насилию в отношении людей или имущества или, по крайней мере, причинить урон, способный вызвать страх. Примерами могут служить атаки, приводящие к смерти или телесным повреждениям, взрывам, авиакатастрофам, загрязнению воды или серьезным экономическим убыткам. Значительные атаки на критическую инфраструктуру могут быть признаны актами кибертерроризма в зависимости от их результата. Атаки, нарушающие функционирование вспомогательных служб или представляющие из себя в основном дорогостоящую неприятность, таковыми не являются».

Данное Деннинг определение весьма полно и включает много аспектов. Она указывает, что атака или «угроза проведения атаки» должны приводить к «насилию в отношении людей или имущества» и что «примерами могут служить атаки, приходящие к смерти или телесным повреждениям». Однако здесь нет упоминания об атаке со стороны негосударственного субъекта. Это означает, что в рамках международного права атака с использованием червя «Stuxnet», проведенная США и Израилем, может рассматриваться как акт кибертерроризма и даже как акт войны.

Кевин Коулман, эксперт в области информационной безопасности, определяет кибертерроризм как:

> «… умышленную подрывную деятельность или угрозу такой деятельности в отношении компьютеров и/или сетей с намерением причинения ущерба или достижения социальных, идеологических, религиозных, политических или аналогичных целей, а также для запугивания кого-либо для достижения указанных целей».

Это определение включает запугивание и использование угрозы «подрывной» деятельности. Также в этом определении не указано, что автором атаки должен быть негосударственный субъект.

Статья под названием «Как нам сдержать терроризм?» в журнале «Information Security Journal: A Global Perspective» определяет кибертерроризм как «деятельность, осуществляемую при помощи компьютеров, сетей, интернета и информационных технологий и имеющую целью помешать политическому, социальному или экономическому функционированию группы, организации или страны или спровоцировать физическое насилие или страх, мотивированная традиционными террористическими идеологиями».

Этот последний пример определения кибертерроризма стоит ближе всего к исходному определению терроризма. Отличие состоит в том, что в данном определении упоминается использование компьютеров и другой IT-аппаратуры для проведения атаки. Как Коулман, так и Деннинг определяют кибертерроризм как действия, направленные против компьютеров, а не совершаемые с их помощью. Это пример того, как определения кибертерроризма могут отличаться друг от друга. Определение, данное в журнале «Information Security Journal», подразумевает, что компьютеры и иная IT-аппаратура используются как средства совершения террористического акта.

ОТХОД ОТ ПОНЯТИЯ «КИБЕРТЕРРОРИЗМ»?

Термин «кибертерроризм» может оказаться неподходящим для описания крупномасштабных кибератак. Слово «терроризм» чаще всего используется в случаях, когда атака привела к человеческим жертвам или разрушению зданий. Учитывая, что этого пока еще не произошло, термин «терроризм» не следует использовать для описания крупномасштабных кибератак. Должно существовать четкое понимание того, понимается ли под термином «кибертерроризм» атака на компьютеры, использование компьютеров или и то, и другое.

В своей статье, опубликованной в 2014 г. в журнале «Perspectives inTerrorism», Ли Джарвис и Стюарт

Макдональд также поставили под сомнение использование термина «кибертерроризм»: «Пожалуй, лучшей иллюстрацией данной проблемы разграничения являются споры о том, является ли описание государственного насилия какого бы то ни было рода в терминах терроризма уместным, полезным или желательным». То же самое справедливо и для кибертерроризма. Мы создаем новые слова и терминологию для уже существующих вещей, и это приводит к путанице: «Это изобилие новых терминологий создает существенные трудности для прояснения таких понятий, как кибертерроризм. Не последнее место среди этих трудностей занимает непоследовательное и взаимозаменяемое использование таких терминов, в результате которого, как показывает [Габриель] Вайман [из Института мира США], "… СМИ зачастую не делают различия между хакингом и кибертерроризмом и преувеличивают угрозу последнего"». Указанное «изобилие новых терминологий» нужно иметь в виду при разработке определения кибертерроризма.

АНАЛОГИЧНОЕ ИССЛЕДОВАНИЕ

Результаты другого исследования Джарвиса и Макдональда, кратко изложенные в статье «Что такое кибертерроризм? Результаты опроса исследователей», также связаны с вопросом описания кибертерроризма. Проведенное ими исследование включало в себя опрос 118 научных работников и фокусировалось на трех проблемах определения: (а) необходимости специального определения кибертерроризма для определяющих политику лиц или для исследователей; (б) основных чертах и составных частях этого понятия; и (в) пользе от применения термина «кибертерроризм» к ряду реальных или потенциальных сценариев. Джарвис и Макдональд приходят к выводу, что, в то время как большинство исследователей считают специальное определение кибертерроризма необходимым для научных работников и определяющих политику лиц, разногласия о содержании этого определения способны привести к более широкому пересмотру понятия «терроризм».

ДОЛЖНО СУЩЕСТВОВАТЬ ЧЕТКОЕ ПОНИМАНИЕ ТОГО, ПОНИМАЕТСЯ ЛИ ПОД ТЕРМИНОМ «КИБЕРТЕРРОРИЗМ» АТАКА НА КОМПЬЮТЕРЫ, ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРОВ ИЛИ И ТО, И ДРУГОЕ.

ПРЕДЛАГАЕМОЕ ОПРЕДЕЛЕНИЕ

Существующие определения кибертерроризма достаточно полны, но оставляют возможность для споров. Поэтому в завершение данного обсуждения я бы хотел повторить мое определение: кибертерроризм – это использование киберпространства негосударственным субъектом в целях нарушения функционирования компьютерных систем, распространения страха или приносящее физический ущерб и, косвенным образом, вред здоровью, либо вызывающее такие перебои в их работе, которые серьезно угрожают репутации жертвы, производимое в политических, идеологических или религиозных целях. Данное определение охватывает наиболее существенные стороны как термина «терроризм» (такие как страх, физическое насилие и спектр мотивов), так и киберизмерения (использование компьютеров для нанесения вреда компьютерам).

ЗАКЛЮЧЕНИЕ

И хотя о кибертерроризме можно писать еще очень много, данная статья проливает свет на сложность определения этого термина и призывает к дальнейшей дискуссии. Есть нерешенные вопросы, касающиеся насилия в киберпространстве и того, является ли кибертерроризмом простое использование интернета террористами. Установление авторства атаки является, вероятно, наиболее трудной задачей и может создать проблемы для правоохранительных органов. Важно отметить, что мы можем так никогда и не прийти к универсальному определению. Достижение приемлемого определения кибертерроризма также зависит от определения термина «терроризм», которое до сих пор является предметом обсуждений.

Но если известные эксперты по терроризму, такие как Вальтер Лакер и Алекс Шмидт, хорошо знакомые с сотнями определений терроризма, не могут прийти к устраивающему всех определению, то кто тогда может? Возможно, термин «кибертерроризм» не следует использовать для описания разрушительной кибератаки. Если нам повезет, мы сможем достичь взаимопонимания, которое позволит улучшить международное сотрудничество по трудному вопросу терроризма и кибертерроризма. Таким образом, определение понятия «кибертерроризм» представляется настоящей дилеммой. □

БАЛТИЙСКОЕ

Эстония, Латвия и Литва подписали исторический документ, призванный согласовать их политику в области кибероборонь

СОТРУДНИЧЕСТВО В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

Витаутас Бутримас,

главный советник Департамента кибербезопасности и информационных технологий Министерства национальной обороны Республики Литва

Подписание 4 ноября 2015 г. меморандума о взаимопонимании (МОВ) представителями трех балтийских государств – Министром экономики и коммуникаций Эстонии, Министром обороны Латвии и Министром национальной обороны Литвы – стало историческим моментом для регионального сотрудничества в области кибербезопасности. Три страны-соседа с богатой историей сотрудничества в традиционных оборонных сферах признали, что они также являются соседями по киберпространству, и договорились официально оформить сотрудничество, начавшееся на неформальной основе за несколько лет до этого. В данной статье описывается процесс, приведший к возникновению этой новой формы сотрудничества в киберпространстве, обсуждается важность данного МОВ, а также рассматриваются некоторые его пункты. Она призвана послужить руководством для других стран, желающих заключить аналогичные соглашения со своими киберсоседями.

ИСТОКИ

Идея МОВ в области киберсотрудничества родилась в конце апреля – начале мая 2007 г. на организованном НАТО семинаре по кибербезопасности, проводившемся Министерством обороны США и компанией Microsoft в штаб-квартире последней в Редмонде, штат Вашингтон. Участники семинара изучали новые возможности использования информационных технологий для защиты на тот момент новейшей операционной системы компании Microsoft «Windows Vista». Организаторы объявили о подписании Соглашения о сотрудничестве в области безопасности с Китаем (а позднее и с Российской Федерацией), в рамках которого властям Китая предоставляется доступ к исходным кодам операционной системы «Microsoft Windows».

Однако атмосфера конференции кардинально изменилась, когда следующий выступающий, эстонец, заявил перед всеми присутствующими: «Моя страна подверглась кибератаке». Участники конференции смотрели друг на друга с удивлением и замешательством. Мы находились на организованной НАТО встрече, в которой принимали участие все высшие руководители в области кибербезопасности, и при этом никто не знал, что делать. В НАТО отсутствовали процедуры реагирования на случай кибератаки на государство, входящее в альянс. Для своевременного реагирования на такое событие не имелось ни соглашений, ни списков контактных пунктов, ни механизмов координирования помощи. Позже тем же вечером в результате телефонных звонков в столицы государств помощь в реагировании на происходившую в тот момент кибератаку на Эстонию была организована и предоставлена. Впоследствии НАТО разработала и предложила странам-участницам альянса возможность подписания МОВ по сотрудничеству в области кибероборонны. Литва стала одной из первых стран, подписавших такой документ летом 2010 г. Идея МОВ овладела умами в Министерстве национальной обороны Литвы, которое также подписало локальный МОВ с национальной Компьютерной группой реагирования на чрезвычайные ситуации (CERT), действовавшей под эгидой Национального управления по регулированию в коммуникационной сфере, а затем и с Министерством иностранных дел. Стало ясно, что иметь письменное соглашение, на которое можно опираться при принятии мер в случае будущих киберинцидентов, – это хорошая идея. Эта идея пустила корни и в других балтийских странах.

ИСТОРИЯ СОТРУДНИЧЕСТВА

В 2009 г. в Риге (Латвия) состоялась первая официальная встреча экспертов в области кибербезопасности из трех балтийских стран. Впоследствии они договорились сделать такие встречи регулярными и проводить их по очереди в трех столицах. В этих встречах принимали участие эксперты в области кибербезопасности из широкого круга организаций, участвующих в обеспечении безопасности киберпространства. Например, в 2012 г. в число представленных на встрече организаций входили три национальные команды CERT, а также министерства транспорта и коммуникаций, обороны, иностранных дел, внутренних дел и полиции. Еще в 2010 г. было решено заложить юридическую основу этих встреч в форме МОВ. Первый рабочий проект меморандума был подготовлен, обсужден и модифицирован на последующих встречах. Этот процесс продолжался несколько лет по причине кадровых изменений и перехода задач по координированию политики в области национальной кибербезопасности к другим ведомствам.

Например, в Латвии координирующее ведомство изменилось с Министерства транспорта и коммуникаций на Министерство обороны, в то время как в Литве последнее изменение произошло в январе 2015 г., когда ответственность за координирование политики была возложена на Министерство национальной обороны в соответствии с принятым в декабре 2014 г. Законом о кибербезопасности. Это последнее изменение обеспечило стабильность в плане ведомственной координации в вопросах окончательного оформления и ратификации проекта МОВ властями каждой страны и подготовки к официальному подписанию, которое было запланировано на весну 2015 г.

Однако официальное подписание пришлось отложить на несколько месяцев, так как дополнительно было необходимо воспользоваться наиболее современными технологиями электронной подписи. Для того чтобы все три национальные электронные подписи на одном и том же документе были признаны каждым подписантом, пришлось преодолеть много технических трудностей. Наконец, после большой работы, проделанной соответствующими центрами сертификации и ведомствами, 4 ноября 2015 г. балтийские министры, отвечающие за координацию национальных политик в области кибербезопасности, подписали Балтийский МОВ по сотрудничеству в области кибербезопасности.

ЧТО ВКЛЮЧАЕТ В СЕБЯ МОВ?

Балтийский МОВ о сотрудничестве в области кибербезопасности состоит из формулировок общих убеждений, разделяемых каждой страной, и соглашений о формах сотрудничества между организациями-участницами. В разделе «принимая во внимание» перечислены следующие общие убеждения:

- Информационные системы и сети являются взаимосвязанными и взаимозависимыми как на уровне одной страны, так и на международном уровне.
- Власти и вооруженные силы различных стран развивают наступательные киберпотенциалы.
- Происходящие из киберпространства киберугрозы включают в себя киберпреступность, атаки на уровне государств, кибершпионаж, а также хактивизм, имеющий политическую, экономическую и/или социальную мотивацию.
- Национальная безопасность включает в себя защиту информационных систем, компьютерных сетей и критической инфраструктуры.
- Для успешного решения всех вышеназванных проблем необходимо международное сотрудничество.

Среди вышеуказанных убеждений отдельного внимания заслуживает то, что кибербезопасность понимается как нечто большее, чем просто реагирование на деятельность киберпреступников и социально мотивированных хактивистов, пытающихся нарушить деятельность IT-систем. Критическая инфраструктура, являющаяся фундаментом, на котором функционирует современное общество, также находится под угрозой из киберпространства. Кибератаки, нарушающие способность систем регулирования контролировать и управлять процессами, происходящими в энергетических, транспортных и водоснабжающих системах, могут принести ущерб благосостоянию общества, экономике и национальной безопасности. Поэтому такая инфраструктура и называется «критической».

Следующим разделом является более конкретный раздел «участники пришли к соглашению». Здесь не содержится ничего нового в плане балтийского сотрудничества в области кибербезопасности; перечисленные здесь виды деятельности имели место на неофициальной основе со времени первой встречи балтийских экспертов по кибербезопасности в 2009 г.

Балтийские эксперты по кибер-безопасности на встрече в Риге (Латвия) в 2012 г.

ВИТАУТАС БУТРИМАС

Процедура электронного подписания Балтийского меморандума о взаимопонимании по сотрудничеству в области кибербезопасности в ходе видеоконференции 4 ноября 2015 г.

МИНИСТЕРСТВО НАЦИОНАЛЬНОЙ ОБОРОНЫ ЛИТВЫ

Разница состоит в том, что МОВ устанавливает юридическую основу этого неформального сотрудничества. Указанные виды деятельности в том числе включают в себя:

- Обмен знаниями и опытом для содействия развитию политик и практик кибербезопасности
- Упор на виды сотрудничества, которые могут снизить риски и уязвимости, связанные с трансграничными зависимостями между независимыми информационными системами, сетями и критической инфраструктурой
- Обмен информацией об обнаруженных киберинцидентах, которые могут повлиять на киберпространства других стран-участниц
- Обмен информацией о раннем обнаружении потенциальных атак, направленных на информационные системы или сети других стран-участниц
- Определение контактных пунктов и обмен контактными данными для обычной и экстренной связи

Перечисленные пункты показывают, что в целях контроля, предотвращения и реагирования на киберугрозы в отношении критической и информационной инфраструктуры друг друга была создана Балтийская организация по взаимодействию в области киберпространства. Определение контактных пунктов полезно, так как каждая сторона знает, «куда звонить» в случае чрезвычайной ситуации. А произведенный заранее обмен контактными данными таких пунктов позволяет избежать путаницы и потенциальных трудностей при реагировании на чрезвычайные ситуации в киберсфере.

НОВЫЙ СПОСОБ ПОДПИСАНИЯ

Данный МОВ можно было подписать при помощи традиционных ручки и бумаги, а затем обменяться полностью подписанными экземплярами. Однако был выбран метод электронной подписи с использованием национальных идентификационных карточек. Это оказалось хорошим способом демонстрации сотрудничества и решения проблем в технической сфере. Понадобилось несколько месяцев, прежде чем удалось добиться того, чтобы различное программное обеспечение по работе с электронными подписями и различные стандарты могли применяться и признаваться всеми сторонами.

И хотя данная работа по решению проблем методом проб и ошибок зачастую вызывала раздражение, она привела и к положительному результату: она предоставила балтийским странам возможность познакомиться с технологиями электронной подписи своих соседей. Решение возникавших проблем углубило технические знания участвовавших в процессе организаций, что может в дальнейшем помочь повысить популярность электронных подписей в балтийских странах.

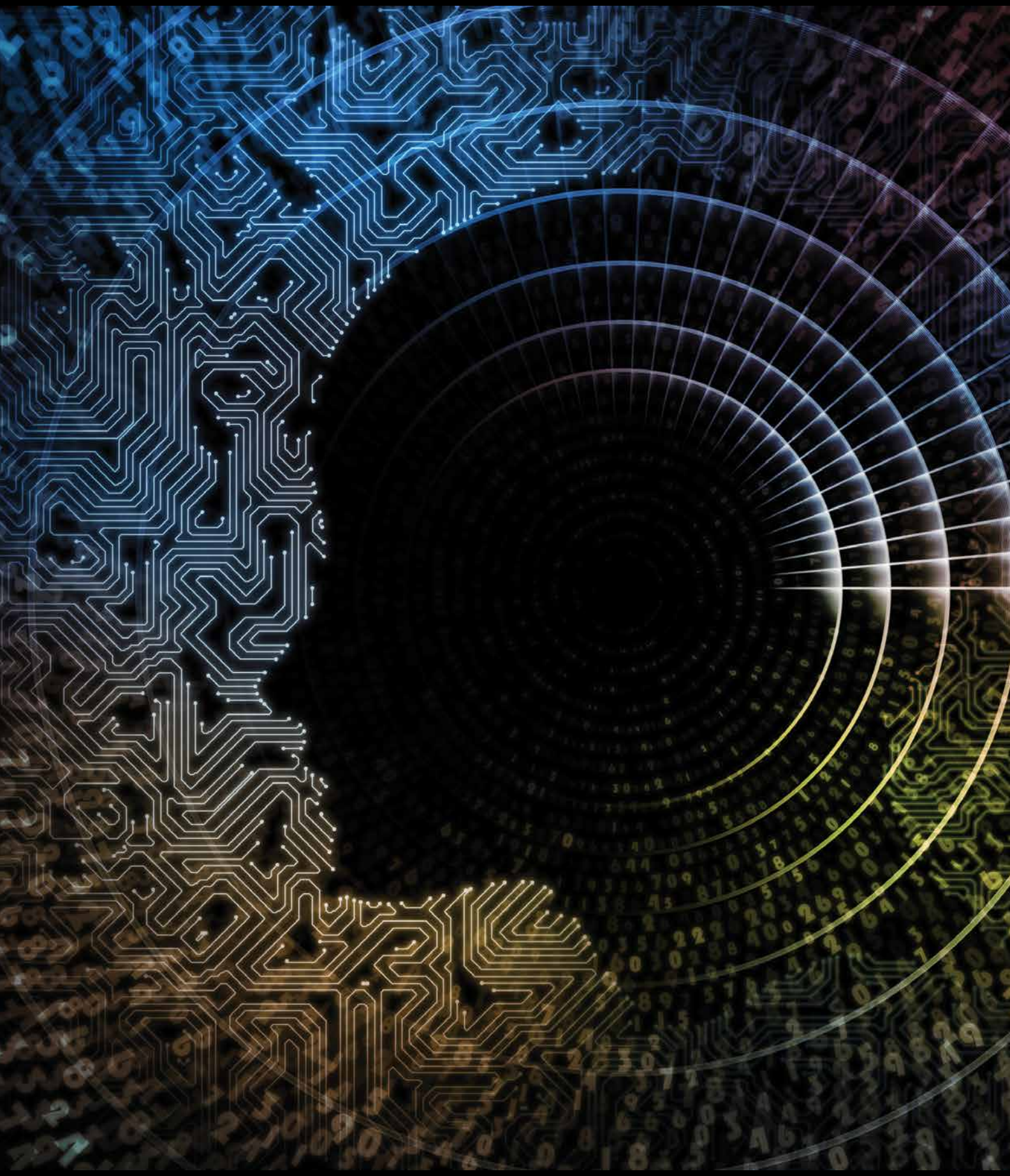
ВЫВОДЫ

Подписание МОВ заняло более пяти лет. Теоретически оно могло занять меньше времени, но совместное действие нескольких факторов очень затянуло процесс. Из процесса работы над МОВ можно извлечь несколько уроков. Во-первых, всегда полезно познакомиться и поговорить со своими киберсоседями. Часто говорят, что в киберпространстве «не существует границ», – это может быть верным в техническом смысле, но неверным в электромагнитной реальности киберпространства. Имеет смысл установить контакт с соседней страной, с которой у вас имеется общая физическая граница. Вы обнаружите, что у вас намного больше общего в плане кибербезопасности, чем вы думали. Вы, вероятно, обнаружите, что благополучие ваших стран зависит от одной и той же инфраструктуры. Энергосети, газопроводы, используемые для коммуникации оптоволоконные кабели, а также интернет-каналы и транспортные системы – все пересекают кибергранницы, что делает одного соседа зависимым от другого в плане предоставления критически важных услуг и доступа к ним. Повреждение в кабеле, обеспечивающем международную связь, или каскадный отказ энергосети влияют не только на ту страну, в которой произошла авария, но и могут повлиять на весь регион.

В стихотворении Роберта Фроста «Починка стены» содержится известная фраза «сосед хорош, когда забор хороший». В этом стихотворении два соседа каждый год встречаются, чтобы «пойти вдоль границы» – вдоль общей стены, разделяющей их участки и формирующей границу между ними, чтобы проверить и отремонтировать ее. Поэт ставит под сомнение необходимость забора. Не нужно беспокоиться о том, что «яблоки» одного соседа упадут между сосен другого. Однако поэт признает необходимость что-то делать с охотниками, проходящими по их землям и наносящими им урон. В сегодняшнем киберпространстве киберсоседям следует «встречаться, чтобы пойти вдоль границы» вместе – для обеспечения взаимной безопасности перед лицом угроз критической инфраструктуре, происходящих из широко используемого и доступного киберпространства.

Это структуры, от которых зависит повседневная жизнедеятельность современного общества. Ни одна организация не может в одиночку защитить эти структуры от их уязвимостей и взаимозависимости, это возможно лишь посредством сотрудничества с другими заинтересованными сторонами. После того как страна «навела порядок в своем доме», подписание МОВ со своими киберсоседями является практичным первым шагом на пути к снижению рисков и укреплению кибербезопасности для всех.

В момент написания настоящей статьи проходит торжественная церемония открытия новых межсистемных связей между энергосистемой Литвы и энергосистемами Польши и Швеции. Критическая инфраструктура, включая энергосети, обладает как трансграничным, так и кибер-измерениями, поскольку для выработки и распределения электроэнергии используются системы регулирования на основе информационных технологий. С учетом последнего события можно предвидеть потребность в присоединении к Балтийскому МОВ двух новых киберсоседей (и партнеров по торговле энергоносителями) Литвы: Польши и Швеции. □



ISTOCK

НОВАЯ УЧЕБНАЯ ПРОГРАММА ПО КИБЕРБЕЗОПАСНОСТИ

КОНСОРЦИУМ «ПАРТНЕРСТВО РАДИ МИРА» ПРЕДЛАГАЕТ ПУТЕВОДИТЕЛЬ ПО ОБРАЗОВАНИЮ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Шон Костиган и Майкл Хеннесси

В заголовках сегодняшних новостей постоянно фигурируют утечки и взломы коммерческих данных, электронное мошенничество, нарушение работы государственных ведомств или критической инфраструктуры, кража интеллектуальной собственности, утечка секретов в сфере национальной безопасности, а также возможность иных разрушений в киберпространстве. То, что ранее являлось сферой радиоэлектронной борьбы, информационной борьбы и экспертов по сетевой безопасности – часто называемой «информационными операциями» или «информационной войной», – ныне трансформируется в намного более широкую сферу, называемую «кибербезопасностью». Эта новая область исследований и практики поставила образовательные учреждения в сфере обороны перед необходимостью работать с тематикой и методами, традиционно находящимися за пределами стандартного образования в сфере обороны.

Ввиду указанной смены парадигмы стремительные и неослабевающие темпы возникновения изменений и вызовов в области кибербезопасности побудили Рабочую группу по новым вызовам безопасности Консорциума «Партнерство ради мира» (ПРМ) поставить задачу по разработке новой учебной программы в области информационной безопасности для военных академий. Разработанная в результате программа была опубликована весной 2016 г. и является плодом работы многонациональной команды, состоящей из выразивших желание участвовать в ее разработке более чем 30 ученых и исследователей из 14 стран, ассоциированных с Консорциумом ПРМ военных академий и институтов по изучению вопросов безопасности. Нашей задачей было создать гибкий и комплексный подход к кибербезопасности с помощью логичной разбивки на конкретные категории в соответствии с уровнем знаний, необходимым для различных групп слушателей, а также включение полезных ключевых ссылок, с тем чтобы каждая страна, заимствующая эту программу, могла адаптировать ее к своим нуждам.

Нахождение необходимого баланса между доступностью, удобством использования и безопасностью является трудной задачей. Новая учебная программа рассматривает различные подходы к оценке угроз и рисков, а также к их идентификации и смягчению правительствами и органами власти на техническом и политическом уровне.

ОБРАЗОВАНИЕ В ОБЛАСТИ БЕЗОПАСНОСТИ И РИСКОВ

Меры безопасности чаще всего принимаются на основе оценки угроз и рисков. В новой учебной программе обоим указанным понятиям уделено много внимания. Однако, говоря простым языком, киберпространство полно угроз, но меры по их уменьшению должны опираться на оценку риска. Международная организация по стандартизации определяет риск как «влияние неопределенности на цели». Это влияние может заключаться в положительном или отрицательном отклонении от ожидаемого. Принимаемые для «обеспечения безопасности» меры должны быть соразмерными допустимому риску. Таким образом, обеспечение безопасности киберпространства влечет за собой ряд соображений по уменьшению рисков и угроз, одновременно поощряя открытое общение в различных типах взаимосвязанных сетей.

Нахождение необходимого баланса между доступностью, удобством использования и безопасностью является трудной задачей. Новая учебная программа рассматривает различные подходы к оценке угроз и рисков, а также к их идентификации и смягчению правительствами и органами власти на техническом и политическом уровне. Она также содержит рекомендуемые передовые практики и сравнительный анализ существующих политик различных государств и организаций.

Задачей данной учебной программы является обеспечить четкую отправную точку для разработки или улучшения преподавания вопросов кибербезопасности высшим военным и гражданским чинам, а также сотрудникам среднего звена. Как и в случае других учебных программ, разработанных Консорциумом ПРМ, данный документ преследует достаточно скромные цели. Он не содержит единой общей схемы курса, которой все должны следовать. Он не является исчерпывающим в плане содержания, деталей или подходов. Однако мы полагаем, что он обеспечит полезный эвристический подход к различным областям, в совокупности обеспечивающим всестороннее введение в спектр вопросов, связанных с национальной безопасностью. Слушатели, не имеющие технической подготовки, найдут здесь введение в тему на разумном уровне сложности и получат понимание того, где и почему требуется техническая глубина. А технически подготовленные слушатели смогут найти здесь полезный обзор уже знакомых им областей, а также введение в более широкий диапазон вопросов международных, национальных и юридических политик и практик.

Предлагаемая учебная программа представлена через четыре широкие темы:

1. киберпространство и основы кибербезопасности;
2. векторы риска;
3. международные организации, политики и стандарты в области кибербезопасности;
4. управление кибербезопасностью в национальном контексте.

Предполагается, что институты, принимающие данную программу, будут работать совместно с экспертами для определения национальных политик и процедур на том уровне детализации, который требуется для целевой аудитории. Механическое знание преходящих технических вопросов может оказаться востребованным, однако целью данной учебной программы является формирование более широкого понимания вызовов в области кибербезопасности во всем их многообразии.

Данная новая типовая учебная программа по кибербезопасности не предлагает единую или рекомендуемую структуру курса. Скорее она является ключевым справочным документом, содержащим общее описание вопросов и тем. Она может служить путеводителем для технических

сотрудников, помогающим им определить свои приоритеты. Или же она может задавать направление вводных курсов для высокопоставленных лиц, принимающих решения в области национальной безопасности, обеспечивая технический контекст, необходимый им для формирования национальной политики.

НАКОПЛЕННЫЙ ОПЫТ

В ходе разработки данной программы мы опросили входящие в Консорциум ПРМ институты и другие военные колледжи, а также проанализировали программы военной подготовки стран-партнеров НАТО и Консорциума ПРМ, чтобы установить содержание учебных программ. Нашей задачей было обнаружение пробелов и общих подходов, выходящих за традиционные рамки правительственных и военных структур. Команда по разработке учебной программы извлекла большую пользу из семинаров, посвященных конкретным странам, которые способствовали более глубокому пониманию разнообразных вызовов, стоящих перед каждой страной в области кибербезопасности.

Участники семинара Военного комитета НАТО на тему кибербезопасности в рамках «Партнерства ради мира» в Грузии. СЕРЖАНТ ПЕРВОГО КЛАССА КЭРРИ ФОКС, ЦЕНТР ИМ. МАРШАЛЛА

В целом, самый большой обнаруженный нами пробел заключается в недостаточном понимании практик уменьшения угроз и рисков в области кибербезопасности со стороны лиц, определяющих политику в области национальной безопасности и обороны. Аналогичный пробел был обнаружен в понимании техническими экспертами базовых рамок национальной политики. Границы между этими двумя группами нельзя описать лишь в терминах положения в военной или гражданской иерархии; таким образом, мы не стали разделять данную типовую учебную программу на блоки в соответствии со служебным положением слушателей.

Были также сделаны дополнительные выводы в нескольких ключевых областях, а именно:

1. Пол – Область кибербезопасности остается преимущественно мужской сферой деятельности. Военные образовательные учреждения имеют возможность сократить этот разрыв.
2. Возраст – Представление о «рождении в цифровую эпоху» продолжает создавать когнитивные трудности для определяющих политику лиц, которые воспринимают кибербезопасность как сферу деятельности молодых людей, а не как критически важную область, в которой должны разбираться руководители любого возраста.
3. Технический потенциал – В странах Восточной Европы существует слишком мало лабораторий по кибербезопасности. Западным военным институтам следовало бы способствовать созданию более современных лабораторий для слушателей.
4. Понимание политики – При обсуждении вопросов национальной кибербезопасности следует принимать во внимание много различных точек зрения, включая культурные. Некоторые страны разработали свою собственную терминологию и сделали осознанный выбор в пользу отказа от использования некоторых широко распространенных терминов
5. Международные различия – Некоторые страны пытаются воспользоваться кажущейся неопределенностью для продвижения своих повесток дня, идущих вразрез с наилучшими интересами демократических стран и глобального обмена информацией.
6. Неоправданный акцент на технических вопросах – Кибербезопасность не является исключительно технической сферой, однако зачастую она рассматривается в качестве таковой как преподавателями, так и принимающими решения лицами. Для того чтобы кибербезопасность стала обычной частью портфеля принимающих решения лиц, требуется определенная степень интеграции этих двух сфер.
7. Правовой контекст – Существует широкий разброс в подходах различных государств к вопросам кибербезопасности в их внутреннем законодательстве. Задача установления авторства – трудности, связанные с установлением источника враждебной, угрожающей или незаконной киберактивности, – добавляет проблем в сферах внутреннего и международного законодательства.
8. Общегосударственный подход – Подходы к решению вопросов кибербезопасности значительно отличаются в разных странах, но кибербезопасность выходит за многие институциональные и организационные рамки. Наилучшие решения должны основываться на комплексном общегосударственном подходе. □

ЭКСТРЕМИЗМ

ISTOCK

ОНЛАЙН В НИГЕРИИ

Страна пытается бороться с умелым использованием социальных сетевых сервисов группировкой «Боко Харам»

ТОММИ ВИКТОР УДО, *Оборонное космическое агентство Нигерии*

Термин «социальные сетевые сервисы» обозначает широкий спектр интернет и мобильных сервисов, позволяющих пользователям участвовать в онлайн-обсуждениях и онлайн-сообществах или делиться пользовательским контентом. К социальным сетевым сервисам обычно относят в том числе такие интернет-сервисы, как блоги, вики, социальные закладки, Твиттер и YouTube. Технологии социальных сетевых сервисов обеспечивают широкий диапазон гибкости, адаптивности и удобства использования.

Террористы и повстанческие группировки – в случае Нигерии это террористическая группировка «Боко Харам» – используют социальные сетевые сервисы в своей противоправной деятельности. Данная статья содержит обзор террористической деятельности «Боко Харам» в Нигерии, обращает внимание на использование группировкой социальных сетевых сервисов, рассматривает инициативы властей по борьбе с использованием социальных сетевых сервисов террористами, а также рассматривает более общие проблемы использования террористами социальных сетевых сервисов.

АКТИВНОСТЬ «БОКО ХАРАМ» В НИГЕРИИ

Группировка *«Джамаату ахлис Сунна Лиддаавати валь-Джихад» (в переводе с арабского «Общество приверженцев распространения учения пророка и джихада»),* более известная под названием «Боко Харам», - это псевдоисламская террористическая группировка, базирующаяся на северо-востоке Нигерии. Название группировки переводится как «западное образование греховно». Таким образом, она выступает против западного образования и западных идеологий и систем, таких как демократия.

«Боко Харам» была основана в 2002 г. Мохаммедом Юсуфом, радикальным исламистским священником из города Майдугури, штат Борно. Секта «Боко Харам» получила известность в 2009 г. в результате участия в межконфессиональном конфликте на севере Нигерии. В том же году Юсуф был убит, а на посту лидера его сменил Абубакар Шекау.

«Боко Харам» ответственна за убийства тысяч ни в чем не повинных граждан, разрушение многочисленных объектов недвижимости, в том числе штаб-квартиры ООН в Абудже, а также похищение граждан, включая школьниц в городе Чибок. Впоследствии деятельность «Боко Харам» распространилась на соседние страны, такие как Чад, Нигер и Камерун.

Группировка присягнула на верность Исламскому государству Ирака и Леванта (ИГИЛ) и намеревается представлять интересы последнего в западноафриканском субрегионе. Хотя «Боко Харам» утверждает, что выступает против западного образования, группировка использует интернет и социальные сетевые сервисы для общения и продвижения своей деятельности.

Использование социальных сетевых сервисов

Как только ИГИЛ признало верность группировки «Боко Харам», последняя расширила свою онлайн-деятельность с использованием приемов, применяемых ИГИЛ. Впоследствии обе группировки стали пользоваться такими платформами, как Фейсбук, Твиттер и YouTube, по причине их дешевизны, удобства и широчайшего охвата, не связанного границами или гражданством. Социальные сетевые сервисы дали «Боко Харам» возможность публиковать сообщения для своей аудитории напрямую без посредников. Как и большинство террористических группировок, «Боко Харам» использует киберпространство – особенно социальные сетевые сервисы – для вербовки, пропаганды, привлечения денежных средств и связи.

Вербовка

При помощи интернета «Боко Харам» получает широкий доступ к восприимчивым молодым людям. Социальные сетевые сервисы используются для обольщения аудитории. Для того чтобы охватить еще больше потенциальных новобранцев и обойти правила медиаплатформ, «Боко Харам» стала обращаться к публике неформально. Например, она обращалась к пользователям Твиттера, которые казались открытыми для идей группировки. Хотя некоторые участвуют в террористических актах ради финансовой выгоды, многих новобранцев из богатых семей и семей среднего класса прельщают экстремальные материалы, распространяемые группировкой в интернете.

Пропаганда

В самом начале «Боко Харам» распространяла свою пропаганду через радиосообщения, а свои видеоматериалы передавала международным СМИ, таким как «Агентство Франс-Пресс», через посредников. Позже группировка перешла к использованию Твиттера, где она размещала видео- и фотоматериалы, показывающие убийства и обезглавливания агентов служб безопасности. Аналогичные клипы размещались на YouTube и переводились на арабский язык, вероятно, с целью охвата большей аудитории. Фотографии и клипы иногда показывают идиллические сцены: деревни и люди, которые, как кажется, живут без страха и говорят о поддержке группировки и преданности ей.

Привлечение денежных средств

По мере эволюции размера, масштабов и структур террористических организаций менялись и их методы привлечения денежных средств и управления ими. Террористические группировки воспользовались стремительным

Женщина несет калебас в лагере для внутренне перемещенных лиц в городе Майдугури (Нигерия) в марте 2016 г. Почти два миллиона людей оказались перемещены в результате войны с «Боко Харам».
РЕЙТЕР

распространением социальных сетевых сервисов для привлечения средств от симпатизирующих им частных лиц и организаций со всего мира. Широкая распространенность доступа в интернет и его относительная анонимность способствуют его использованию фандрейзерами террористов. Имели место случаи, когда при помощи социальных сетевых сервисов ни в чем не повинных граждан заманивали и похищали, чтобы затем, в некоторых случаях, потребовать выкуп с родственников или сотрудников похищенного. Группировка также использует социальные сетевые сервисы для привлечения денежных средств в форме предоплаченных карт и для крупномасштабных краудфандинговых схем с использованием электронных кошельков. Полученные деньги используются для вербовки, мотивирования и обучения добровольцев; для закупки вооружения, боеприпасов и взрывчатых веществ; для распространения пропаганды; а также для проведения научно-исследовательских работ.

Связь

Социальные сетевые сервисы становятся основным средством поддержания связи друг с другом, а также с традиционными СМИ и каналами связи общего пользования. Социальные сетевые сервисы позволяют сегодняшнему поколению в полной мере воплотить концепцию «свободного рынка идей», выдвинутую английским поэтом Джоном Мильтоном, где кажется, что ложь и правда публикуются одновременно новыми пользователями сервисов. «Боко Харам» использует

На постере, размещенном Армией Нигерии в северо-восточном городе Дамбоа в феврале 2016 г., изображены сто разыскиваемых подозреваемых из «Боко Харам». AFP/GETTY IMAGES

такие коммуникационные платформы, как Skype, групповые чаты, Instagram, Твиттер, Фейсбук и WhatsApp. Террористическая группировка выбирает эти каналы связи благодаря их низкой стоимости, легкости использования и анонимности. Эти средства связи могут использоваться всеми, вне зависимости от того, близко или далеко они находятся, а также позволяют террористическим группировкам связываться с ИГИЛ для обмена идеями или получения денежных средств.

БОРЬБА С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНЫХ СЕТЕВЫХ СЕРВИСОВ ТЕРРОРИСТАМИ

Сбор финансовой разведывательной информации

Программа по внедрению банковских проверочных номеров (БПН) усиливает безопасность банковских операций и способствует сбору финансовой разведывательной информации в стране. Данная правительственная инициатива способствует выявлению отмываемых денежных средств и обмену информацией о возникающих рисках. Применяемые в Нигерии уникальные БПН упрощают задачу банков по установлению личности вкладчиков вне зависимости от количества имеющихся у них счетов. Данная программа привела к сокращению практики использования вкладчиками различных персональных данных для отмывания денежных средств через различные банки и счета. При помощи БПН банки могут отслеживать необычную активность на счетах. Основное направление деятельности состоит в выявлении и закрытии точек сбора/накопления/распределения денежных средств, используемых преступными и террористическими организациями. БПН позволяют правоохранительным органам концентрироваться на получателе денежных средств, а не только на их источнике.

Программа кибербезопасности

Федеральное правительство Нигерии поддержало принятие национальной программы кибербезопасности, состоящей из Политики и стратегии кибербезопасности и из Закона о киберпреступлениях. Закон о киберпреступлениях обеспечивает эффективные, единые и всеобъемлющие правовые, нормативные и институциональные рамки для запрета, предотвращения, обнаружения и уголовного расследования киберпреступлений в Нигерии, а также для наказания за них. Данный закон обеспечивает защиту критической информационной инфраструктуры страны и способствует кибербезопасности и защите компьютерных систем и сетей, электронных коммуникаций, данных и компьютерных программ, интеллектуальной собственности и права на неприкосновенность частной жизни. Он обязывает операторов связи сохранять все данные о трафике и абонентскую информацию, принимая во внимание закрепленное в конституции право личности на неприкосновенность частной жизни, и принимать надлежащие меры для защиты конфиденциальности данных при их сохранении, обработке или отборе.

Компьютерная группа реагирования на чрезвычайные ситуации

Нигерийская компьютерная группа реагирования на чрезвычайные ситуации была создана для мониторинга случаев нарушения безопасности в национальном киберпространстве и для реагирования на них – как проактивного, так и реактивного. Проактивная служба защищает киберпространство Нигерии в ожидании атак, проблем или иных событий. Предоставляемые услуги включают в себя наблюдение за технологиями, услуги по обнаружению вторжений, оценку уязвимостей и тестирование на возможность проникновения. Реактивные службы созданы для ответа на запросы об оказании помощи в борьбе с любыми угрозами или атаками на информационные системы в киберпространстве страны. Они включают в себя анализ инцидентов, реагирование на инциденты по месту их возникновения, координирование реагирования на инциденты, поддержку реагирования на инциденты, сбор улик и криминалистический анализ.

Стратегические онлайн-нарративы

Стратегический онлайн-нарратив – это заявление об идентичности, причинах и намерениях, объединяющее правительство, народ и вооруженные силы Нигерии в их борьбе против терроризма. Оно последовательно доводится до членов «Боко Харам», широких слоев населения и силовых структур. Предназначенный для членов «Боко Харам» и постоянно распространяемый контрнарратив продвигает умеренную форму ислама. В нем говорится, что Святой Пророк никогда не убивал невинных детей и не похищал женщин в целях распространения дела ислама. Он также призывает их быть правоверными мусульманами и сдаться или подчиниться властям, которые примут их и будут хорошо с ними обращаться. Нарратив, предназначенный для силовых структур, укрепляет их боевой дух и напоминает военнослужащим, что они воюют за правое дело.

Кризисные коммуникационные центры по социальным сетевым сервисам

Кризисные коммуникационные центры могут отслеживать активность в социальных сетевых сервисах. В их работе принимают участие представители гражданского общества, прессы, групп энтузиастов/активистов в области социальных сетевых сервисов, молодежи и неправительственных организаций, обменивающиеся идеями и предоставляющие сведения, которые можно использовать для противодействия идеологии насильственного экстремизма.

Обнаружение онлайн-активности террористов и борьба с ней

Силовые структуры Нигерии обладают современными технологиями, содействующими сбору информации о террористах: они позволяют производить законный перехват электронных коммуникаций, если существуют достаточные основания подозревать, что их содержание необходимо для уголовного расследования или судебного разбирательства.

Разъяснительная и предупредительная работа с населением

Правительство Нигерии призывает граждан страны проявлять бдительность и добровольно предоставлять властям информацию, которая может помочь силовым структурам предотвратить нападения «Боко Харам». Сходным образом, в интернете распространяются советы, как узнать террориста и предоставить соответствующим органам информацию, которая может привести к его аресту. Платформы социальных сетевых сервисов заполнены специально созданными театральными и комедийными сценками, музыкальными клипами, рекламными песенками, а также свидетельствами сдавшихся в плен и дерадикализованных членов «Боко Харам» и документальными фильмами. Кроме того, в районах, подконтрольных «Боко Харам», а также на встречах по военно-гражданскому взаимодействию на операционном и тактическом уровнях и в области здравоохранения и инфраструктуры распространяются листовки и фактологические пресс-релизы.

ВЫЗОВЫ В ОБЛАСТИ СОЦИАЛЬНЫХ СЕТЕВЫХ СЕРВИСОВ

Меняющаяся тактика

Как выяснилось, в долгосрочной перспективе трудно различить сочувствующих, сторонников и истинных террористов. Серьезной проблемой для органов безопасности является выявление лиц, намеренно или невольно жертвующих деньги. Сложно получить доказательства использования принадлежащих террористам денежных средств, когда они переводятся через интернет. Социальные сетевые сервисы можно использовать для выявления связей, но найти доказательства все равно трудно.

Баланс между неприкосновенностью частной жизни и безопасностью

Иногда властям было бы выгодно заблокировать доступ гражданина к веб-сайтам или серверам, которые используются террористами. Однако такую политику сложно реализовать на практике, принимая во внимание право на свободу в интернете.

Отказ в доступе известным террористам

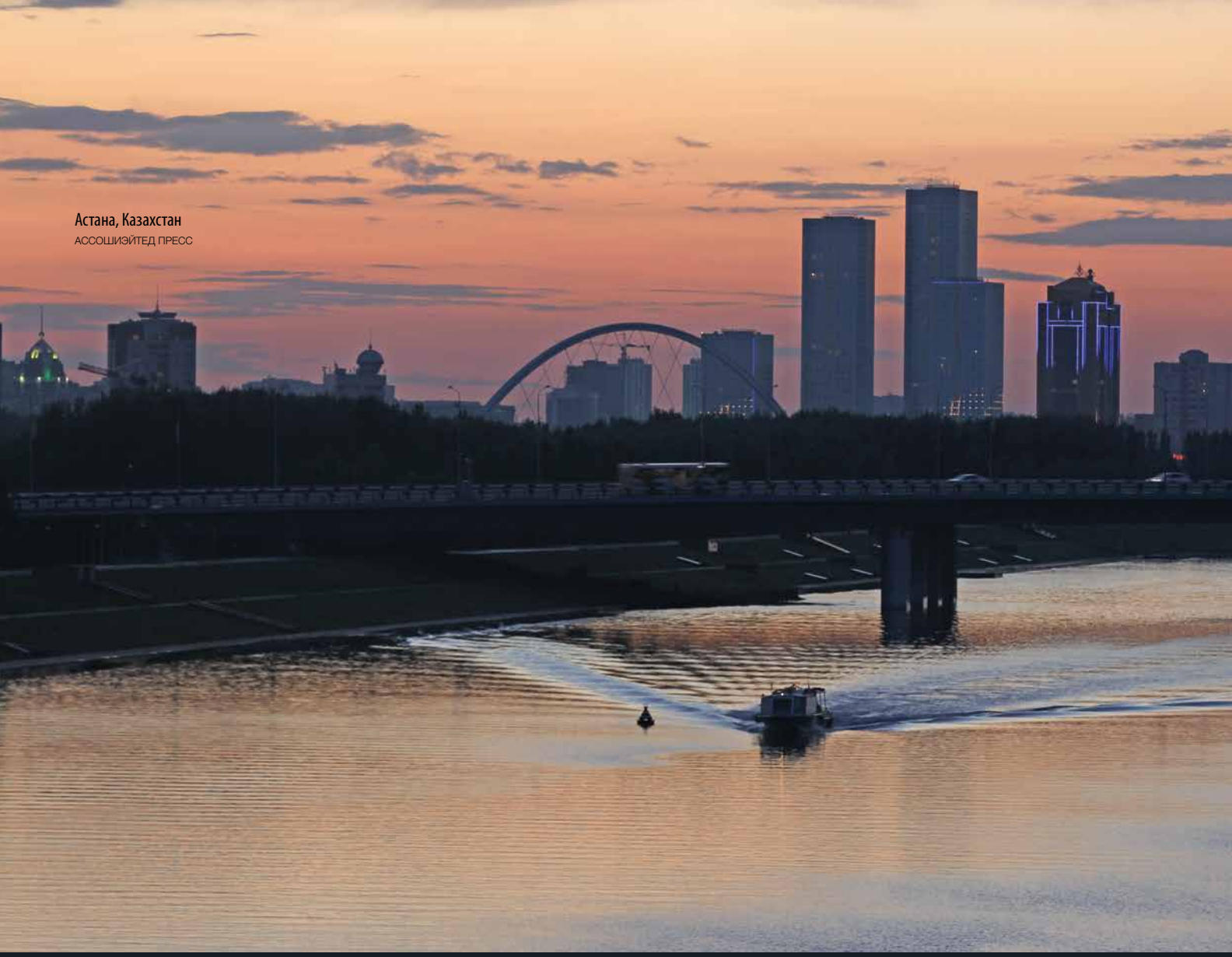
YouTube, Твиттер и Фейсбук – вот лишь некоторые из платформ социальных сетевых сервисов, используемых для пропаганды террористическими группировками, такими как «Боко Харам». Когда известный лидер террористической организации по типу Абубакара Шекау размещает в социальных сетевых сервисах пропагандистское видео, всегда трудно добиться согласия владельцев или администрации этих платформ отказать террористам в использовании их платформ/серверов, даже в случае, когда пользователем является известный террорист.

Заключение

Террористы из «Боко Харам» в Нигерии, как и другие террористические организации, постоянно пытаются использовать социальные сетевые сервисы для решения задач по вербовке, пропаганде, привлечению денежных средств и связи. Правительство Нигерии учитывает риски, присущие киберпространству. Поэтому оно должно серьезно относиться к киберрискам, чтобы граждане страны имели возможность и дальше пользоваться всем потенциалом революции в области информационных и коммуникационных технологий. В этих условиях власти страны намерены бороться с угрозами, отстаивать и поддерживать открытость киберпространства, а также находить баланс между безопасностью, с одной стороны, и неприкосновенностью частной жизни и фундаментальными правами, с другой.

Правительство Нигерии постоянно реализует новые инициативы по противодействию использованию социальных сетевых сервисов террористами через всеобъемлющие программы национальной кибербезопасности, использование данных финансовой разведки для отслеживания денежных средств, а также создание коммуникационного центра для борьбы с террористической идеологией и радикализацией. Другие инициативы включают в себя слежку в интернете, цензуру, кибероперации, а также образовательную работу с населением и повышение его осведомленности.

Некоторые вызовы по-прежнему существуют, и усилия по их преодолению продолжаются. Эти вызовы включают в себя способность идентифицировать денежные средства, переводимые через социальные сетевые сервисы, а также цели этих переводов. Другим вызовом является нахождение баланса между свободами граждан в интернете и национальной безопасностью. Наконец, сложность получения согласия владельцев и администрации платформ социальных сетевых сервисов на отказ в доступе известным террористам представляет собой еще один вызов. □



Астана, Казахстан
АССОШИЭЙТЕД ПРЕСС

КАЗАХСТАН АДАПТИРУЕТСЯ К КИБЕРЭРЕ

СТРЕМИТЕЛЬНЫЕ ПЕРЕМЕНЫ СТАВЯТ ПЕРЕД ЭТОЙ ЦЕНТРАЛЬНОАЗИАТСКОЙ СТРАНОЙ ЦЕЛЫЙ КОМПЛЕКС ВЫЗОВОВ

Анна Гусарова, Казахстанский институт стратегических исследований

Влияние, которое информационные и коммуникационные технологии оказывают на все сферы человеческой жизни, привело к возникновению новых уязвимостей. Произошли коренные перемены в структуре социальных отношений и в роли государств. На международной арене расцвел кибершпионаж, ставящий под вопрос эффективность международного правового режима. Изменения в балансе сил в виртуальном пространстве может привести к изменениям в геополитическом балансе сил. Государства не только действуют в киберпространстве напрямую, но и активно пользуются возможностями дискредитировать своих политических и экономических соперников в реальном мире. Системы обороны и критическая инфраструктура стали уязвимыми.

В течение последних нескольких лет впечатляющими темпами шла интеграция Казахстана в глобальное информационное сообщество. Недостаточное внимание к новым возможностям, а также к рискам и угрозам, может повредить развитию страны и отбросить ее на периферию международных отношений. В этом смысле существует необходимость в постоянном мониторинге и ситуационном анализе с целью правильного понимания стремительных и фундаментальных изменений в обстановке.

IT-РЕВОЛЮЦИЯ

Стремительное развитие информационных технологий привело к возникновению новой конкурентной среды в международных отношениях, в которой кибертехнологии играют ключевую роль в повседневной жизни. Именно здесь проходит передний край борьбы за научное, техническое, политическое и экономическое превосходство.

Разработка цифровых технологий – это дорогая отрасль, требующая огромных инвестиций не только в оборудование и цифровые носители информации, но и в обучение персонала. В результате традиционные ключевые игроки в сфере международных отношений, такие как США, Великобритания, Китай и в определенной степени Россия сохранили лидирующие позиции.

Интернет больше не является лишь надежной системой для передачи электронных сообщений. Сегодня интернет – это место, где в прямом смысле слова миллионы людей живут и работают, продают и покупают товары, организуют онлайн-аукционы, создают семьи, обсуждают интересные темы, развлекаются и различными способами самовыражаются. Другим важным результатом развития кибертехнологий стало уменьшение возможностей охраны государственных секретов. Случай Эдварда Сноудена является примером этой уязвимости.

Потенциал международного кибершпионажа и международное проникновение в национальные секторы киберпространства подняли вопрос о жизнеспособности принципа государственного суверенитета. Эти новые параметры уязвимостей поставили проблему регулирования киберпространства в рамках международного права.

Существует два основных подхода. Они не являются взаимоисключающими, а, скорее, по-разному расставляют акценты. Первый подход основан на глобальной деятельности под руководством Совета Европы по разработке общих стандартов безопасности на основе Конвенции о киберпреступности, которые могли бы заложить основу для противодействия киберугрозам и регулирования межгосударственных отношений в данной сфере. Второй подход уделяет главное внимание национальным системам кибербезопасности на основе потенциалов и интересов, которые могли бы задать глобальные правила поведения в киберпространстве. Действия технологически развитых государств говорят о том, что на данный момент доминирующим является второй подход.

КАЗАХСТАН И ЦЕНТРАЛЬНАЯ АЗИЯ

Государства Центральной Азии остаются на периферии распространения информационных технологий. Тем не менее цифровые технологии начинают играть все более важную роль в государственных и общественных сферах жизни стран региона. В то же время страны Центральной Азии зачастую подвергаются преступным кибератакам, в основном имеющим своей целью финансовое мошенничество.

По данным сервиса Kaspersky Security Network, Казахстан стал объектом 85% всех интернет-атак на страны региона, по сравнению с 8% Узбекистана, 4% Кыргызской Республики, 2% Туркменистана и 1% Таджикистана. Большинство кибератак были направлены на правительственные веб-сайты с целью получения финансовой информации. Считается, что большинство преступлений в киберпространстве совершается хакерами, относящимися к местным организованным преступным группировкам, пытающимся добыть ценные финансовые и промышленные данные.

По данным Всемирного банка, ежемесячно в Казахстане интернетом пользуется более 10 млн. человек, или около 60% населения. В сельских районах уровень проникновения интернета существенно ниже, около 30%. Однако тренд направлен резко вверх, так как доля интернет-пользователей среди населения выросла с 0,5% в 2000 г. до 15% в 2008 г. и 41% в 2011 г. Среднестатистический пользователь является лицом мужского пола в возрасте от 15 до 35 лет с доходами не ниже среднего – или же студентом.

Электронная коммерция отвечает лишь за 0,45% всего розничного рынка в Казахстане; однако эксперты полагают, что в 2015 г. с использованием электронной торговли было осуществлено до 4% розничных продаж на общую сумму 3 млрд. долл. США. В Обзоре ООН по уровню развития электронного правительства за 2014 г. Казахстан занял 28-е место среди 193 стран по уровню развития электронного правительства, 23-е место по электронному участию и 23-е место по оказанию онлайн-услуг.

Возникновение электронного правительства способствует изменениям в отношениях между обществами и их властями в направлении демократизации, а также к сокращению административных расходов. В то же время сетевое взаимодействие (в своем кибернетическом и социальном измерении) привело к утрате правительствами монополии на осуществление властных полномочий, определяемых как возможность влиять на деятельность и поведение и задавать тенденции социального поведения. Очевидно, что способность – в первую очередь техническая – влиять на информационное наполнение делает возможным манипулирование общественным сознанием.

Кибербезопасность является относительно новой темой в Казахстане, а защита данных приобрела огромное значение для государства и частных лиц. Тенденции развития киберпространства в Казахстане включают в себя:

- Облегчение доступа к информационным ресурсам (интернет, цифровое телевидение, мобильная связь, современные технологии).
- Рост компьютерной грамотности и вовлеченности граждан в информационную сферу (электронное обучение, электронные банковские услуги, электронные деньги, электронная коммерция, мобильные терминалы приема платежей «Pay-me», покупки через интернет).
- Преобразование многих сфер общественной жизни на основе широкомасштабного прогресса в области информационных и коммуникационных технологий (ИКТ) (появление электронного правительства, Центр оперативного контроля, унифицированные системы контроля).
- Интеграция в глобальное информационное пространство.

ПРОНИКНОВЕНИЕ КИБЕРТЕХНОЛОГИЙ

Электронное правительство

Казахстан является лидером по предоставлению электронных государственных услуг. Из 675 правительственных служб 236 доступны через портал электронного правительства e-gov.kz, а 77 доступны онлайн (около 11,4%).

В 2010 г. был создан общедоступный портал электронных государственных закупок www.goszakup.gov.kz, находящийся под управлением товарищества с ограниченной ответственностью «Центр электронной коммерции». В 2011 г. начали работать две системы: система электронного лицензирования частных компаний и объединенная система «электронного нотариата» и «электронного акимата» для районных администраторов. С 2012 г. онлайн-платформа www.egov.kz объединяет базы данных Министерства здравоохранения, Министерства внутренних дел и ЗАГСов. На этом же веб-сайте можно оплатить 21 вид госплатежей, 16 видов госпошлины, четыре вида налогов, а также штрафы за нарушение ПДД. В апреле 2012 г. был выдан 1 млн. цифровых подписей – электронных подписей, идентифицирующих граждан.

Согласно правительственной статистике, к маю 2012 г. число пользователей портала egov.kz выросло в 122 раза, с 25-30 посещениями в день. 6% населения пользуется услугами электронного правительства, и эта доля растет быстрыми темпами. По данным Программы по развитию информационных и коммуникационных технологий, в 2013 г. на развитие портала было выделено 5,2 млрд. тенге (34,5 млн. долл. США), а в 2014 г. – 9,7 млрд. тенге (64,5 млн. долл. США).

Казахстан создал Национальный инфокоммуникационный холдинг «Зерде» – государственную компанию, задачей которой является развитие современных информационных и коммуникационных технологий. В стадии разработки находится национальное «облако», в котором будет размещена государственная IT-инфраструктура страны.

Электронная коммерция

Значительная глубина проникновения интернета в Казахстане привела к стремительному росту электронной коммерции. Объемы интернет-торговли выросли на 300% в 2011 г. и на 180% в 2012 г. Согласно правительственной статистике, годовой оборот электронной торговли в 2012 г. приблизился к 400 млн. долл. США (0,7% рынка), а в иностранных магазинах граждане Казахстана тратят более 1,3 млрд. долл. США.

Рынок электронной коммерции Казахстана состоит из более чем 500 интернет-магазинов. По данным Национального банка Казахстана, по состоянию на апрель 2013 г. гражданам страны было выдано 13 млн. кредитных карт. В интернет-торговле успешно участвуют такие фирмы, как АО «Казкоммерцбанк», «Эйр Астана», АО «Казахстанские железные дороги», «Сульпак», «Технодом» и «Меломан».

Кибервызовы

Рука об руку с положительными тенденциями в сфере ИКТ Казахстана идут растущие вызовы в области информационной и кибербезопасности. Казахстан занимает 18-е место в мире по количеству получаемого спама и седьмое по опасности веб-серфинга. По данным опубликованного в декабре 2014 г. информационного бюллетеня «Лаборатории Касперского», «в течение 2013 г. IT-инфраструктура 92% организаций в стране по крайней мере один раз подвергалась внешней кибератаке, а 66%

компаний столкнулись с внутренними угрозами информационной безопасности».

Сегодня растущую угрозу представляют мобильные устройства. У 85% компаний в Казахстане был хотя бы один инцидент в области информационной безопасности. Лишь за первую половину 2013 г. «Лабораторией Касперского» было зарегистрировано 53 тыс. уникальных образцов вредоносного кода, направленного на мобильные устройства.

Кроме того, в 2013 г. кибератаке подвергся каждый второй пользователь в стране (55,5%). В 2013-2014 годах в Казнете было зарегистрировано 76 млн. случаев встречи с вредоносным программным обеспечением. Чаще всего с киберугрозами сталкиваются жители Алматы, Атырау и Шымкента (западная и южная части страны).

Развитие глобального киберпространства общественными институтами является гигантским шагом на пути к устойчивому развитию. Однако по сообщениям участников интернет-конференции iProf-2012, безопасность государственных веб-сайтов в Казахстане оставляет желать лучшего и требует значительного внимания (99% сайтов не способны отразить атаки хакеров). Хорошим примером такой уязвимости может служить имевшая место в 2012 г. хакерская атака на официальный веб-сайт Министерства культуры и информации.

На сегодняшний день скимминг мало распространен в Казахстане, однако количество кибератак с использованием этого метода растет, как и во всем мире. Так, например, как сообщает веб-сайт «TengriNews», в 2013 г. несколько граждан Румынии и Молдовы были задержаны в Алматы за использование скимминговых устройств для кражи данных из картоприемников банкоматов. Также стремительно растет число кибератак с использованием мобильного банкинга и случаев компьютерного мошенничества на фондовой бирже.

Имело место несколько кибератак на электронное правительство, как то: попытка хакеров уничтожить сайт e-gov.kz, а также официальную блог-платформу правительства Казахстана (2009 г.); атака на веб-сайт Национального космического агентства Казахстана (2010 г.); атака на веб-сайт Комитета по правам интеллектуальной собственности Министерства юстиции (2012 г.); а также атака на официальный веб-сайт Агентства по борьбе с экономической и коррупционной преступностью, т.е. финансовой полиции (2012 г.).

НОРМАТИВНО-ПРАВОВАЯ БАЗА В КИБЕРСФЕРЕ

Инициативы в области кибербезопасности в Казахстане зачастую исходят от главы государства. В частности, в ходе юбилейного саммита Шанхайской организации сотрудничества президент Казахстана Нурсултан Назарбаев предложил ввести новое понятие «электронных границ» и создать в рамках организации специальное подразделение для защиты от интернет-агрессии. Он также ввел в международное право термин «электронный суверенитет». На 66-й сессии Генеральной Ассамблеи ООН в 2011 г. Назарбаев предложил ускорить принятие Договора о глобальной кибербезопасности.

Казахстан и другие страны-участницы ОБСЕ выстроили нормативно-правовую базу для киберпространства. В последние годы в Казахстане принят целый ряд законов об электронном правительстве, электронных деньгах, электронной коммерции, интеллектуальной собственности и так далее.

На концептуальном уровне не существует четкого понимания разницы между «информационным пространством» и «киберпространством». В нормативно-правовой терминологии Казахстана практически не встречается префикс «кибер» (киберпространство, кибербезопасность, киберпреступность, кибервойна). Официальная терминология использует в этих понятиях более широкий префикс «информационный» (информационное пространство, информационная безопасность, информационная война). Однако оба варианта считаются эквивалентными в свете их широкого использования в СМИ и обычной речи.

В 2013 г. президент подписал указ, утверждающий государственную программу «Информационный Казахстан – 2020», призванную создать условия для перехода Казахстана к информационному обществу. Программа была разработана совместными усилиями Министерства транспорта и коммуникаций и заинтересованных экспертов. Ее целями являются повышение эффективности государственного управления и доступности информационной инфраструктуры, а также развитие национального информационного пространства. Ожидается, что посредством внедрения ИКТ будут решены задачи по оптимизации государственного управления, а также создано открытое и «мобильное правительство». Однако в программе не рассматриваются вопросы информационной безопасности.

Следует отметить, что кибербезопасность и киберпреступность в Казахстане существуют по большей части в экономической плоскости: оценка материальных и интеллектуальных ресурсов компаний, отношения с партнерами по корпоративным или производственным вопросам и состояние институциональных связей. Это подтверждает уголовный кодекс Казахстана, согласно которому экономические преступления с применением высоких технологий бывают двух разновидностей: «неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ» и «неправомерное изменение идентификационного кода абонентского устройства сотовой связи».

В целом, данные с 2004 по 2010 годы ясно показывают интенсивный рост этого вида преступности: 26 преступлений в 2004 г., 713 в 2005, 1 437 в 2006, 1 622 в 2008, 2 196 в 2009 и 2 423 в 2010. Хотя не существует общедоступных данных за последующие годы, высока вероятность того, что данная тенденция к росту сохранилась и позже.

Казахстан является лидером по предоставлению электронных государственных услуг. Из 675 правительственных служб 236 доступны через портал электронного правительства e-gov.kz, а 77 доступны онлайн.

Астана, Казахстан
АССОШИЭЙТЕД ПРЕСС

Новый проект уголовного кодекса проясняет уголовные преступления против безопасности информационных систем и содержит десять поправок, проясняющих в числе прочих такие преступления, как неправомерный доступ; неправомерная модификация или распространение информации; компьютерный саботаж; создание, использование или распространение вредоносных компьютерных программ и программных продуктов; а также нарушение правил использования информационных систем.

На институциональном уровне президент в 2010 г. дал поручение по созданию Компьютерной группы реагирования на чрезвычайные ситуации Казахстана (KZ-CERT) для защиты от киберугроз, внедрения информационных и коммуникационных технологий и обеспечению кибербезопасности. Ее функции включают анализ информации, вирусов, кодов безопасности и программ «ботнетов» из доменов зоны .kz, а также нарушения законодательства (порнография, насилие, нарушение авторских прав и так далее) пользователями Казнета. KZ-CERT оказывает содействие в реагировании на атаки «отказ в обслуживании» (DoS, DDoS), взлом онлайн-ресурсов, внедрение и распространение вредоносного программного обеспечения, фишинг, вирусы и ботнеты.

ОСВЕДОМЛЕННОСТЬ ОБ IT-УГРОЗАХ

Низкая осведомленность о киберугрозах среди IT-пользователей затрудняет защиту национального киберпространства Казахстана. По данным «Лаборатории Касперского», около 17% пользователей мобильных устройств не предпринимают никаких специальных действий для защиты паролей доступа к финансовым и/или платежным службам, а 39% пользователей во всем мире предпочитают использовать лишь один или лишь незначительное количество различных паролей для всего спектра посещаемых ими сайтов. Осведомленность о киберугрозах критически низка: лишь 6% респондентов знакомы с понятиями уязвимостей и атак «нулевого дня», 21% в некоторой степени знакомы с этими понятиями, а 74% совершенно не знакомы с ними. Например, лишь 4% респондентов были осведомлены о трояне Zeus/Zbot, заразившем 196 стран по всему миру, в то время как 73% были совершенно не осведомлены о нем.

Низкая осведомленность о киберугрозах ведет к несоблюдению базовых правил информационной безопасности. Кроме того, более половины компаний в Казахстане (52%) не выделяют денег и ресурсов на разработку политики в области IT-безопасности и покупку лицензионных версий антивирусных программ. Таким образом, в Казахстане наблюдается острая необходимость повысить уровень осведомленности об угрозах среди общественных институтов, частных предприятий, а также среди обычных интернет-пользователей. С апреля 2016 г. сотрудники правительственных ведомств будут обязаны оставлять свои смартфоны и планшеты на пропускных пунктах для минимизации утечки конфиденциальной информации через WhatsApp и другие мессенджеры. Например, в США существуют программы обучения старшеклассников и их учителей, а также широкой публики в области информационной безопасности, а федеральные служащие проходят обучение информационной безопасности.

НЕДОСТАТОЧНАЯ КВАЛИФИКАЦИЯ В ОБЛАСТИ IT

На сегодняшний день в Казахстане наблюдается острый дефицит квалифицированных IT-специалистов. Обладающих техническими навыками сотрудников трудно удержать по причине высокого спроса на эти навыки на мировом рынке труда. В 87% казахских компаний работают IT-специалисты, не способные адекватно оценить новые угрозы и предотвратить их реализацию. Между тем, по данным «Лаборатории Касперского», корпоративная IT-инфраструктура, которую можно заразить через мобильные устройства сотрудников, является основной мишенью кибератак. Казахстан должен лучше привлекать и удерживать высококвалифицированных профессионалов в области информационной безопасности.

Одной из основных задач по усилению кибербезопасности страны является развитие партнерства между государственным и частным секторами. На сегодняшний день сотрудничество между государством и частными компаниями в области кибероборонs находится на критически низком уровне. Также имеет место недостаток сотрудничества между общественными институтами и частными компаниями в сфере компьютерных технологий и разработки программного обеспечения. Для эффективной кибербезопасности требуется дальнейшее развитие сотрудничества между правительством и партнерствами с участием государственных и частных организаций, т.е. операторами критической инфраструктуры и государством.

НОВЫЕ МЕРЫ КИБЕРБЕЗОПАСНОСТИ

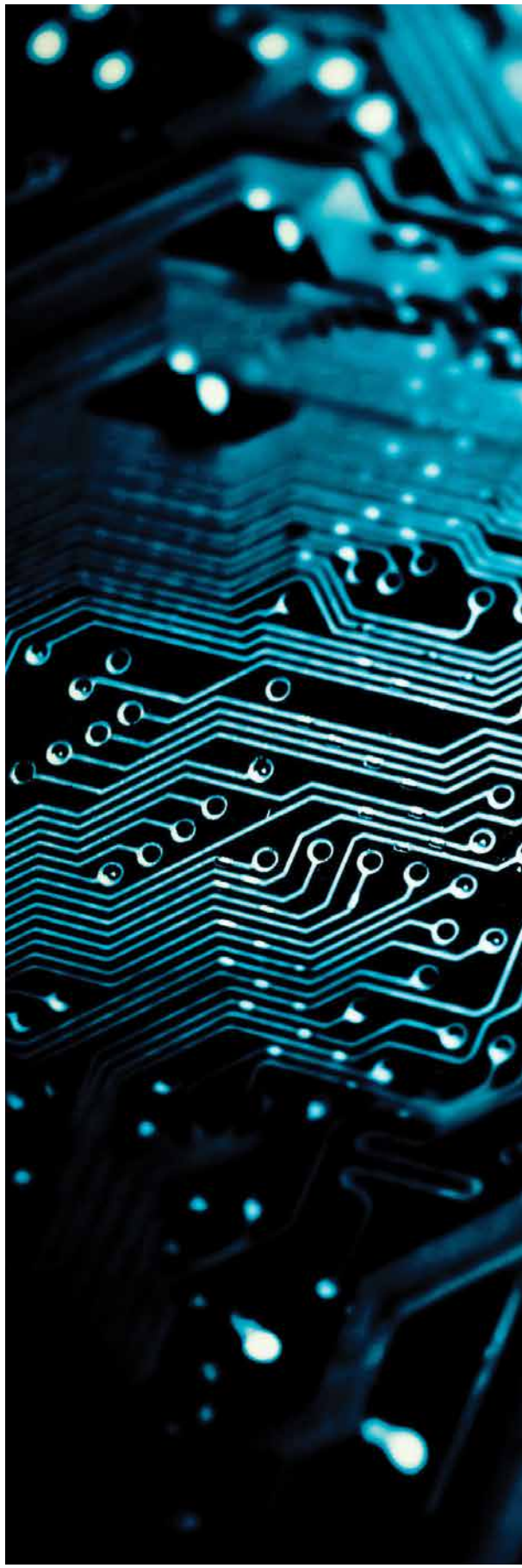
Вступивший в силу 1 января 2016 г. новый закон Казахстана «О связи» вводит национальные сертификаты безопасности для пользователей интернета. Все операторы связи обязаны осуществлять пропуск трафика с использованием протоколов, поддерживающих шифрование, с применением сертификата безопасности, за исключением трафика, шифрованного средствами криптографической защиты информации. Целью национального сертификата безопасности является защита жителей Казахстана внутри страны с использованием протоколов шифрованного доступа к зарубежным интернет-ресурсам.

На пути реализации данного закона на всей территории страны есть много трудностей, а стоимость проекта составит миллионы долларов США. Однако по мере того как Казахстан вступает в киберэру, власти должны предпринять шаги по защите своих сетей, критической инфраструктуры и граждан от расширяющегося спектра новых угроз. □

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ МОЛДОВЫ

Контакты, доверие и коммуникация являются ключом к мощному киберпотенциалу

Наталья Спину,
руководитель молдавского Центра кибербезопасности,
ГП «Центр специальных телекоммуникаций»



Сегодняшнее киберпространство несет в себе неисчислимые риски для безопасности частных компаний и общественных институтов, делая их легкими целями для кибератак со стороны групп «хактивистов», террористических организаций и поддерживаемых государством хакеров. Прошло время, когда организация могла выдержать этот натиск без посторонней помощи. Коллективные меры реагирования, основанные на обмене информацией, могут помочь организациям лучше подготовиться к этим новым вызовам и сделать их более устойчивыми к последним.

В большинстве случаев обмен информацией носит добровольный характер и основывается на конкретной потребности или на доверии, выстроенном в течение длительного времени. В некоторых развитых странах были реализованы законодательные инициативы, поощряющие и поддерживающие такую деятельность, в то же время снижающие риски для частного сектора через использование властей страны в качестве доверенной третьей стороны. Именно в этой области имеют место партнерства между государственным и частным секторами.

В Республике Молдова не существует партнерств между государственным и частным секторами в сфере киберпространства. Поэтому обмен информацией обычно происходит на нерегулярной основе. Неформальный характер этого процесса существенно сказывается на способности компаний и правительственных организаций решать проблемы, создаваемые кибератаками. Именно это обстоятельство сыграло роль в серьезных инцидентах, недавно произошедших в Молдове (массовые заражения шифровальщиком «CTB-Locker», утечка базы данных «Starnet» и другие).

ISTOCK

Президент Молдовы Николае Тимофти идет мимо почетного караула в ходе участия во встрече Восточного партнерства Евросоюза в Праге. Исполнительная власть Молдовы стоит во главе усилий по повышению кибербезопасности страны. АССОШИЭЙТЕД ПРЕСС

Обмену информацией между частным и государственным секторами и внутри самого частного сектора мешает множество факторов, в том числе:

- пробелы в национальном законодательстве;
- отсутствие точек соприкосновения между частными компаниями и общественными институтами;
- незнание структуры и задач государственных институтов, участвующих в обеспечении кибербезопасности, а также того, как и кому сообщать о противоправных действиях или случаях нарушения безопасности;
- нехватка квалифицированных специалистов;
- отсутствие совместных учений.

В соответствии с действующим законодательством, на сегодняшний день в Молдове существует семь организаций, которые принимают участие в противодействии киберугрозам и должны производить обмен киберинформацией на политическом, техническом и гражданском уровне:

- ***Высший совет безопасности –*** консультативный орган, контролирующий реализацию политики правительства в области национальной безопасности.
- ***Служба информации и безопасности –*** специализированный орган государственной безопасности, отвечающий за противодействие киберугрозам в масштабе всей страны.
- ***Министерство информационных технологий и связи –*** департамент, разрабатывающий и реализующий государственную политику в области информационных и коммуникационных технологий (ИКТ), включающей в себя киберпространство.
- ***Генеральная прокуратура –*** отвечает за координацию действий и уголовное преследование за совершение киберпреступлений.

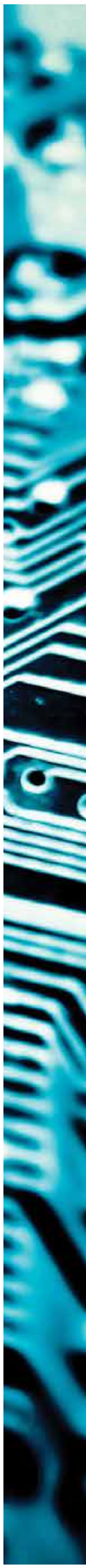
- ***Центр по борьбе с киберпреступностью –*** подразделение полиции, специализирующееся на расследовании киберпреступлений и аресте подозреваемых в их совершении.
- ***Национальный центр по защите персональных данных –*** автономный орган власти, отвечающий за соблюдение законодательства в сфере обработки персональных данных.
- ***Центр кибербезопасности CERT-GOV-MD –*** государственная компьютерная группа реагирования на чрезвычайные ситуации.

Центр кибербезопасности CERT-GOV-MD – это структура правительственного уровня, занимающаяся развитием национальной кибербезопасности. На него возложена ответственность за решение сложных киберпроблем. В последние годы CERT-GOV-MD осуществил ряд мероприятий, направленных на улучшение обмена киберинформацией в масштабах всей страны:

- ***Создание национальных и международных контактных пунктов.*** В июне 2013 г., во исполнение указа премьер-министра, CERT-GOV-MD выступил с инициативой, в соответствии с которой органам государственной власти предлагалось обмениваться информацией об угрозах и уязвимостях с CERT-GOV-MD и сообщать ему о любой злонамеренной деятельности. Данная инициатива заложила дополнительный основополагающий элемент в механизм обмена информацией в государственном секторе, а на техническом уровне определила ответственных лиц в органах власти. Еще одна задача была выполнена в 2014 г., когда CERT-GOV-MD стал аккредитованным членом «Trusted Introducer» - организации, объединяющий европейские компьютерные группы реагирования на чрезвычайные ситуации. Это способствовало установлению прямых и надежных каналов связи с международным сообществом кибербезопасности.
- ***Укрепление доверия.*** С 2013 г. по 2015 г. CERT-GOV-MD организовал цикл международных конференций и семинаров, собравших вместе представителей частных компаний, правительственных структур и университетов, а также ведущих экспертов в области кибербезопасности, которые помогали устранить барьеры непонимания и налаживали взаимоотношения.
- ***Поощрение коммуникации.*** Участвуя одновременно в практической деятельности по противодействию киберинцидентам, затрагивающим безопасность государства, в разработке политики, а также в местных, национальных и международных группах и проектах, CERT-GOV-MD выработал уникальное и целостное понимание вопросов кибербезопасности в Молдове. Это делает возможной передачу критически важной информации о наиболее острых проблемах от наиболее удаленных органов власти к высшим руководителям страны.

Кибербезопасность требует всестороннего подхода. Политическая воля, вовлеченность в процесс в масштабах всей страны и участие ведущих экспертов являются ключом к созданию условий, в которых государственные институты могут обеспечить необходимый уровень кибербезопасности.

Кибербезопасность требует всестороннего подхода. Политическая воля, вовлеченность в процесс в масштабах всей страны и участие ведущих экспертов являются ключом к созданию условий, в которых государственные институты могут обеспечить необходимый уровень кибербезопасности. Успешное достижение этой цели зависит от контактов, доверия и коммуникации. Именно эти компоненты определяют роль и миссию Центра кибербезопасности CERT-GOV-MD в национальном обмене киберинформацией в Молдове. □



Господство в киберпространстве

В ХОДЕ ВОЕННЫХ ОПЕРАЦИЙ

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ДАЕТ ЕВРОПЕЙСКОМУ КОМАНДОВАНИЮ ВООРУЖЕННЫХ СИЛ США ТАКТИЧЕСКОЕ ПРЕИМУЩЕСТВО

Европейское командование вооруженных сил США

Нападай на противника, когда он не готов; выступай, когда он не ожидает.
— Сунь Цзы, «Искусство войны»

По мере того как информационный век продолжает коренным образом менять наш мир, понимание киберпространства в рамках знакомого набора терминов и логичных тактических принципов становится критически значимым для победы. Сегодня, как и на протяжении всей истории, для того чтобы победить, успешные командиры должны находить ключевые моменты во времени и пространстве и пользоваться ими. Операции в киберпространстве не являются исключением. Понимание потенциального влияния, которое киберпространство может оказать на проведение операций, разработка общих принципов для понимания и управления этим влиянием, а также создание сил для проведения кибермиссий могут дать значительное преимущество.

Киберпространство – это новый уровень сложности, на котором игроки могут оказывать воздействие на весь спектр военной и гражданской деятельности, так как информационные системы приобретают все большее значение практически во всех аспектах военных операций. Чтобы одержать победу в XXI веке, командиры должны быть знакомы с возможностями и ограничениями своих систем при помощи методологии, вносящей четкость и ясность в понимание возможного воздействия киберпространства.

Понимание значительной потенциальной роли киберпространства играет критическую роль в удержании киберпревосходства: речь идет о способности эффективного использования систем в нужное время и с нужной интенсивностью. Киберпространство – это искусственно созданная среда, состоящая из географии, аппаратного обеспечения, логических сетей (программного обеспечения, приложений), профилей пользователей (имен пользователей и их логинов), а также людей. Сегодня доступ в интернет есть почти у 40% населения Земли, по сравнению с менее чем 1% 20 лет назад. Поэтому поддержание безопасности в киберпространстве становится все более сложной задачей. По данным веб-сайта «InternetLiveStats», количество пользователей интернета выросло в десять раз с 1995 г. по 2001 г., достигло 1 млрд. в 2005 г., 2 млрд. в 2010 г. и 3 млрд. в 2015 г. На веб-сайте Международного союза электросвязи говорится, что почти у половины из 7 млрд. человек, живущих на планете, есть доступ в эту операционную среду.

А с учетом грядущей волны интернета вещей, включающего лампы, фото- и видеокамеры и автомобили, это число достигнет 20 или 30 млрд. – в три-пять раз больше, чем число людей на планете. Так как все сети тем или иным образом взаимосвязаны, это означает, что командующие будут сталкиваться с растущими вызовами по осознанию изменений, сохранению киберпревосходства и проведению операций.

Разработка общих принципов по улучшению понимания киберпространства даст командирам возможность быстро осознать происходящие изменения и встать во главе перемен. В «Основополагающей концепции совместных операций – 2020» описывается, как будущие противники могут начать более умело использовать киберпространство и продолжать бросать вызов нашей способности проведения операций. Командиры должны обладать методологией, позволяющей быстро связать воедино географию, аппаратное обеспечение, логические сети, профили и людей в рамках простых общих принципов, способствующих осознанию изменений и дающих возможность действовать, так как и методология, и общие принципы имеют жизненно важное значение для победы.

Одним из возможных подходов является использование модели анализа местности, известной как «секторы наблюдения и ведения огня, укрытие и маскировка, препятствия, ключевой рельеф, пути подхода», – термин, с которым знакомо большинство военных стратегов. Точно так же, как эти факторы должны быть проанализированы в отношении миссии, типа операции, уровня командования, состава сил и

ожидаемых от противника вооружения и оборудования, командиры могут использовать эти же принципы в киберпространстве. Фактор «секторов наблюдения и ведения огня» может быть использован для определения потенциальных районов боевого соприкосновения, в которых системы и платформы ударных сил наиболее подвержены наблюдению и кинетическому или некинетическому огневому воздействию. Понимание этих опасных районов поможет защитить военные силы и средства.

Важность фактора «укрытие и маскировка» в размещении тактической военной техники аналогична важности профилей пользователей в защите доступа в сеть. Процесс укрытия и маскировки тактической техники не представляет трудностей, а вот логические сети, профили и люди требуют хорошо продуманных совместных действий для снижения рисков и уязвимости. В условиях боевой обстановки под фактором «препятствий» обычно понимаются природные или искусственно созданные особенности рельефа, останавливающие, затрудняющие, замедляющие или перенаправляющие движение. Эти же самые понятия применимы и к киберпространству. Понимание того, как создавать препятствия при помощи аппаратного обеспечения, например, межсетевых экранов и прокси-серверов, и программного обеспечения, например, цифровой идентификации и двухфакторной аутентификации, необходимо для нарушения способности противника влиять на операции.

Определение «ключевых или решающих точек на местности» – это больше, чем просто соотнесение техники с физическим местоположением; сюда также входит выявление ключевых систем, таких как противоракетная оборона, управление огнем и электростанции, играющих жизненно важную роль в успешном проведении операций. Каждая из указанных систем является примером логической сети и может быть ключевой точкой на местности. Люди и профили пользователей также могут быть ключевыми точками на местности, так как могут служить в качестве точек доступа к различным системам. Выявление ключевых точек на местности позволяет командирам превратить каждую особенность рельефа в именованную зону потенциальной угрозы и задать расположение соответствующих наблюдательных позиций.

Наконец, понимание «путей подхода», также известных под названием «вектора атаки», играет центральную роль в понимании слабых сторон своего подразделения. Командиры, анализирующие пути подхода к своим киберсистемам, включая те, что могут повлиять на аппаратное обеспечение, логические сети, профили пользователей и людей, лучше подготовлены к развертыванию сил кибермиссии и определению оборонительной тактики в ходе проведения операций. Использование факторов оценки местности «сектора наблюдения и ведения огня, укрытие и маскировка, препятствия, ключевой рельеф, пути подхода» для анализа географии, аппаратного обеспечения, логических сетей, профилей пользователей и людей повышает осведомленность и помогает командирам прийти к

Украинский солдат принимает участие в проводившемся в 2014 г. семинаре «Киберусилие», являющемся частью инициативы Европейского командования вооруженных сил США по улучшению коллективной кибербезопасности союзников и партнеров НАТО. МАЙОР ДЖЕЙСОН РОССИ, ВОЕННО-ВОЗДУШНЫЕ СИЛЫ США

лучшему пониманию того, как действовать быстрее и встать во главе перемен, что обеспечивает преимущество им и их подразделениям.

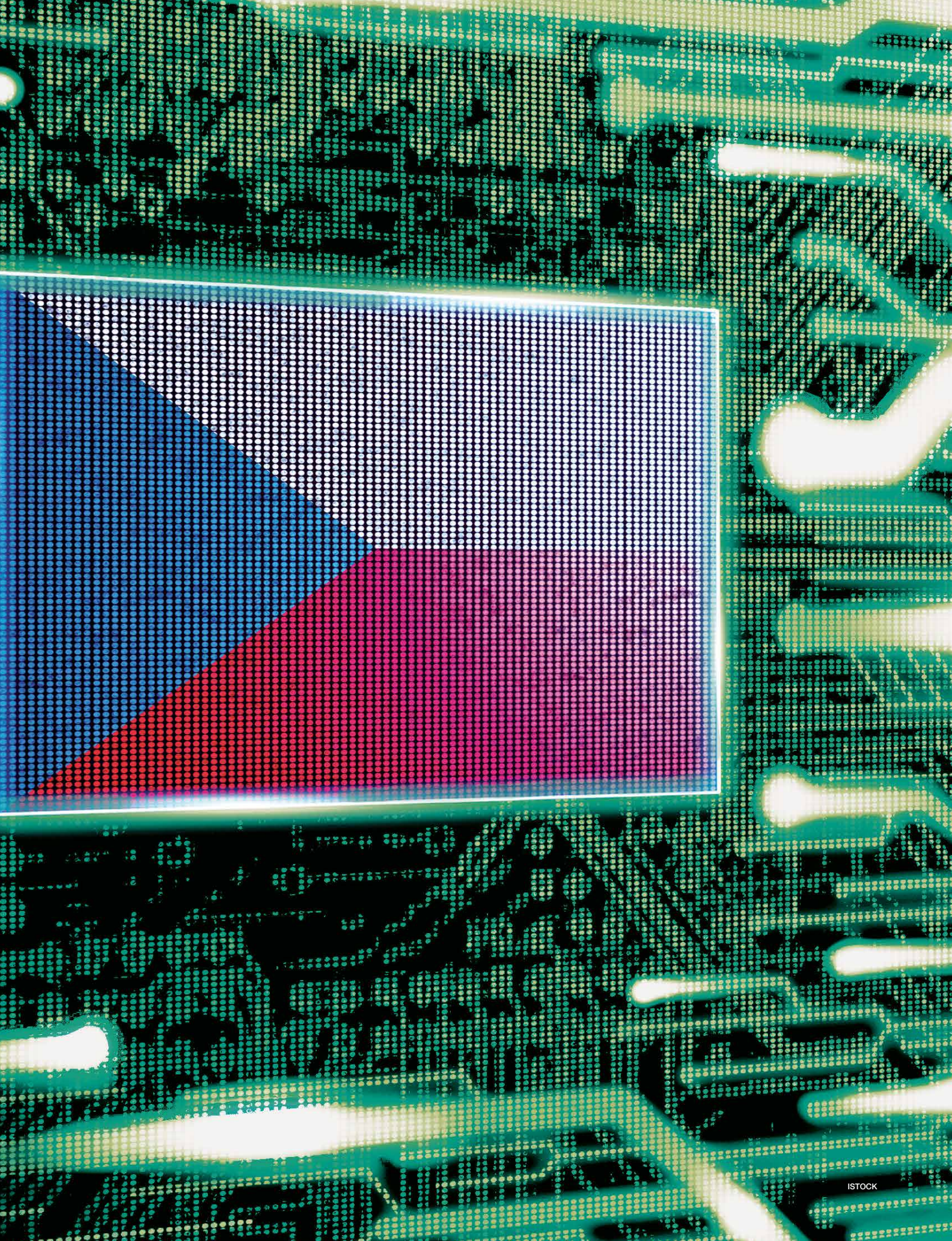
Предоставление формированиям возможности действовать в качестве составной части сил кибермиссии имеет принципиальное значение для победы. По мере того как количество угроз продолжает возрастать, командирам следует стимулировать подразделения «ввязываться в кибердраку» для максимизации эффективности наших сил кибермиссии. В «Основополагающей концепции совместных операций» говорится, что «способность действовать в соответствии со своими намерениями через доверие, расширение возможностей и понимание» является составной частью совместной стратегии, призванной обеспечить нашим командирам возможность действовать в сложной обстановке и в составе объединенных сил для предотвращения конфликта, формирования условий безопасности и побед в войнах.

Для достижения господства в киберпространстве в ходе проведения операций требуются понимание среды, общие принципы, позволяющие осознать изменения и встать во главе перемен, а также способность обеспечить каждому военнослужащему возможность участия в работе сил кибермиссии. Командиры будут продолжать корректировать свой процесс принятия военных решений и свои тактические расчеты, проигрывая в уме ход конфликтов с помощью определения этапов и порядка действий, их разветвлений и последующих действий для выявления ключевых точек на местности, ключевых задач и ключевых этапов принятия решения. По мере того как киберпространство продолжает расти, командирам следует принять общую систему координат, которая даст возможность их подразделениям осознать изменения и встать во главе перемен для достижения побед в XXI веке. □

ПОДХОД К КИБЕРБЕЗОПАСНОСТИ СО СТОРОНЫ ЧЕШСКОЙ РЕСПУБЛИКИ

КОМПЛЕКСНЫЕ УЧЕНИЯ ЯВЛЯЮТСЯ НЕОБХОДИМЫМ ИНСТРУМЕНТОМ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА

Дэниэл П. Багге и Мартина Улманова
Национальный центр кибербезопасности Чешской Республики



ISTOCK

Благодаря стремительным темпам технологических инноваций людям, не являющимся специалистами в сфере кибербезопасности, трудно в полной мере понять угрозы, исходящие от компьютерно грамотных террористов и преступников. Это особенно верно в отношении правительств и частных организаций, которые в большинстве своем не осознают возможных последствий от обращения этих технологических инноваций против них. Новые методы и изощренность атак, а также растущий круг их целей являются частыми объектами открытых докладов и обсуждений. Общество, получающее такую информацию, ожидает от своих властей создания жизнестойкого и безопасного киберпространства. Но как могут власти оставаться на шаг впереди развивающихся технологий, особенно учитывая, что бюрократические системы обычно имеют низкую скорость реакции на вызовы, с которыми принимающие решения лица большей частью незнакомы?

Следовательно, чтобы быть в курсе технического прогресса и иметь возможность быстро адаптироваться к новым угрозам, необходимо быть хорошо подкованным в киберсфере. Однако эксперты в области информационных технологий (IT) и работники технологической сферы не могут в полной мере представлять себе все влияние IT-продуктов и решений на национальную безопасность. Технический персонал оперативного уровня и менеджеры в области кибербезопасности незнакомы с процессами принятия политических, дипломатических и стратегических решений. Они зачастую живут в узком мире технологий. Схожим образом, высшее руководство, сотрудники правоохранительных органов и лица, определяющие политический курс, сталкиваются в свой работе со значительными трудностями без знания технологических последствий и воздействий киберинцидентов.

Добиться того, чтобы квалифицированные технические специалисты понимали стоящие перед правительством вызовы, а представители власти углубили свое понимание возможных последствий инцидентов, связанных с киберпространством, является трудной задачей. Ввиду ограниченности по времени и нехватки ресурсов на национальном уровне для проведения крупномасштабной и своевременной образовательной работы, наилучшим способом решить эту задачу являются учения по кибербезопасности.

Они не только имеют непосредственное влияние на набор навыков их участников, но также одновременно позволяют оценить выученные уроки. Учения по кибербезопасности можно разделить на несколько типов: командно-штабные, технические, гибридные или процедурные, с небольшими наложениями между указанными типами. Все типы учений позволяют их участникам поработать над важными аспектами реагирования на инциденты, такими как командная работа, обмен информацией и межорганизационное сотрудничество.

В то время как широкой публике легко представить себе технические учения – группа IT-специалистов и компьютерные группы реагирования на чрезвычайные ситуации ведут борьбу за инфраструктуры друг друга и защищают свои периметры при помощи клавиатур и экранов, – лица, принимающие решения на более высоких уровнях, не могут разрешить все трудности, связанные с киберкризисом, при помощи нажатия одной кнопки на клавиатуре. Высшее руководство не сталкивается с кибервызовами на ежедневной основе и может оказаться неспособным произвести адекватную оценку кризиса и дать правильные указания низшим эшелонам. Таким образом, учения, направленные на процессы принятия решений, являются уникальной возможностью познакомить высшее руководство с соответствующими вопросами кибербезопасности. Вместе с использованием реалистичных сценариев это является наилучшим способом просветить высшее руководство в отношении важности кибербезопасности и ее актуальности в плане национальной безопасности. Можно возразить, что обладания необходимым техническим потенциалом достаточно для разрешения инцидента или кризиса в сфере кибербезопасности, но это не так. Хотя технические / оперативные эксперты по кибербезопасности владеют нужными навыками и новейшими технологиями, без соответствующего командования и управления они бесполезны.

Более того, существует еще одна тенденция, о которой мы должны знать в этот цифровой век. Параллельно с разрывом в знаниях между техническим персоналом и принимающими решения лицами нам приходится иметь дело с различными способностями и навыками у более молодого и у более старшего поколения. В то время как более молодые люди хорошо знакомы с открытым интернетом и находят его легкодоступным, многие руководители высшего

В ЧЕШСКОЙ РЕСПУБЛИКЕ ПРИЗНАЕТСЯ ПОТРЕБНОСТЬ В НЕПРЕРЫВНОМ ОБУЧЕНИИ КАК ТЕХНИЧЕСКИМ НАВЫКАМ, ТАК И КОММУНИКАЦИОННЫМ И ПРОЦЕДУРНЫМ АСПЕКТАМ КИБЕРБЕЗОПАСНОСТИ.

звена не могли и представить себе интернет-век в начале своей карьеры.

ЧЕШСКИЙ ОПЫТ И ПРАКТИКА

В Чешской Республике признается потребность в непрерывном обучении как техническим навыкам, так и коммуникационным и процедурным аспектам кибербезопасности. Поэтому Национальный центр кибербезопасности (НЦКБ) регулярно принимает участие в учениях на международном уровне, включая «Учения по кризисному реагированию» и учения «Киберкоалиция», проводимые НАТО; учения «Сомкнутые щиты», организованные Центром передового опыта в области коллективной кибероборонь; и учения «КиберЕвропа», организованные Европейским агентством сетевой и информационной безопасности. Кроме участия в указанных международных учениях, НЦКБ организовал и принял участие в двух национальных учениях в 2015 г.: в командно-штабных учениях, предназначенных для стратегических лидеров и принимающих решения лиц, и в технических учениях для администраторов и специалистов в области информационных и коммуникационных технологий.

Проведенные в Праге в июне 2015 г. «Учения по принятию стратегических решений» и «Учения по урегулированию киберкризисов» были совместной инициативой Управления национальной безопасности Чешской Республики, Европейкой инициативы по кибербезопасности (Эстония) и Европейского оборонного агентства. В ходе учений исследовалась способность государства принимать решения и эффективно использовать имеющиеся ресурсы для противодействия киберкризису. В ходе данного трехдневного мероприятия почти 40 участников, представляющих правительство страны, вооруженные силы, разведывательные службы, частный сектор, полицию, прокуратуру и другие правоохранительные органы, имели дело с обостряющимся и вполне реалистичным сценарием. Сценарий был разбит на шесть фаз и на непрерывные сюжетные линии с представлением различных форм киберугроз. У каждой рабочей группы был свой набор информации, что требовало от участников эффективного сотрудничества. Результаты, включая графическую визуализацию учений, были тщательно проанализированы, а затем с основными заинтересованными лицами и участниками было проведено итоговое мероприятие. Целью учений было не выявить победителя, а определить пробелы и недостатки в процессе принятия решений и произвести проверку каналов связи в ходе основанного на реальных сценариях кризиса, который обострился от незначительных инцидентов до военного вмешательства и чрезвычайного положения.

В сентябре 2015 г. перед НЦКБ была поставлена задача по разработке и проведению специально разработанных командно-штабных учений, основанных на реальной угрозе, для Министерства обороны США и Кибернетического командования США в Вашингтоне, округ Колумбия. Помимо прочего, в учениях рассматривалась кибер- и информационная война, кампании по кибершпионажу, предвыборная пропаганда, утечка чувствительной информации, а также взлом компьютерных программ и данных. Целью учений было повышение осведомленности о последствиях в области политики и национальной безопасности, связанных со значительными киберинцидентами, и рассмотрение трудностей в процессе принятия решений. Учения были оценены их участниками как успешные и будут

проведены повторно в 2016 г. Специально разработанные командно-штабные учения были обновлены в начале 2016 г. и проведены в июне в штабе командования по трансформации объединенных вооруженных сил НАТО в Норфолке. Учения также проводились в рамках Саммита по кибербезопасности Вышеградской четверки, организованного председательствующей в данной структуре Чешской Республикой, в Вашингтоне, округ Колумбия.

Участники международных учений по кибероборонe «Сомкнутые щиты – 2016».
ХАНС-ТООМАС СААРЕСТ, СИЛЫ ОБОРОНЫ ЭСТОНИИ

Чешская Республика хочет и может делиться своим опытом в сфере проведения учений по кибербезопасности на стратегическом уровне. В конце 2015 г. НЦКБ провел специальные командно-штабные учения для студентов магистерской программы в области исследований по безопасности и стратегии Университета им. Масарика в городе Брно.

ТЕХНИЧЕСКИЕ УЧЕНИЯ

Первые национальные технические учения в области кибербезопасности, «КиберЧехия – 2015», были проведены в прошлом году. Они были организованы Управлением национальной безопасности, являющимся для НЦКБ вышестоящим органом, совместно с Институтом компьютерных наук (ИКН) Университета им. Масарика. Они проводились в ИКН в специальной виртуализированной учебной среде, называемой «киберполигоном». Противники взаимодействовали в рамках этой уникальной, изолированной от внешнего мира компьютерной системы, в которой можно протестировать любой программный код или решение без риска для внешних сетей. Целью учений было подвергнуть участников реальным кибератакам. По сценарию учений команды являлись частью вымышленных сил быстрого реагирования Чешской Республики. Командам была поставлена задача оказать помощь атомной электростанции, чьи информационно-коммуникационные системы подверглись массивной атаке. Хотя обороняющиеся команды соревновались друг с другом, учения поощряли обмен информацией и сотрудничество.

Это были первые технические учения, в которых могли принимать совместное участие представители ключевых органов власти и других компетентных структур Чешской Республики. В дальнейшем, в марте 2016 г., была проведена еще одна стадия учений. Аналогичная возможность участия была предоставлена частным компаниям, представляющим критическую информационную инфраструктуру, особенно в энергетическом секторе. Чтобы подчеркнуть важность такого рода учений, премьер-министр Чешской Республики посетил их лично. Они были беспрецедентны как по своему масштабу, так и по тому, что позволили участникам и наблюдателям приобрести опыт защиты важного объекта критической инфраструктуры. Учения «КиберЧехия» были первой проверкой данного сценария, который также предназначен для использования в научных исследованиях, а также государственными учреждениями и частными компаниями. Участвовавшие в учениях команды не только реагировали на атаки и технические проблемы, но и давали оценку потенциальным правовым и медиапоследствиям. Эти два аспекта – правовой и медиа – включаются во все национальные учения, так как считаются неотъемлемыми элементами разрешения возможных кризисов и необходимы для обеспечения кибербезопасности.

На сегодняшний день было проведено два вида учений. Однако накопленный в ходе их проведения опыт помог НЦКБ понять, что пришло время гибридного подхода. Это означает соединение технических учений с командно-штабными учениями стратегического уровня и с традиционными процедурами кризисного реагирования для обеспечения готовности всех органов национальной безопасности к крупномасштабному кризису. Сюда входят органы антикризисного управления, разведывательное сообщество, органы национальной безопасности, а также заинтересованные лица из вооруженных сил, научного сообщества и частного сектора.

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ УЧЕНИЙ

В прошлом учения в основном делились на две сферы: технические и командно-штабные. Однако эти сферы тесно переплетены в плане трудностей и инструментов,

необходимых для решения стоящих задач. Недостаточно обучать только технический персонал или только высшее руководство при помощи специфических учений в соответствии с их родом деятельности. В условиях киберкризиса им придется координировать ответные меры и действия и осуществлять обмен информацией не только горизонтально, но и вертикально. Следует поощрять проведение учений, в рамках которых эти два мира сотрудничают друг с другом. Кроме того, следует привлекать частный сектор, научное сообщество и СМИ. СМИ являются значимой заинтересованной стороной, обладающей ключом к разрешению киберкризисов. Они играют решающую роль не только в ходе информирования общественности о происходящих киберинцидентах, но и в формировании общественного мнения в целом. Это имеет важное значение в свете растущей роли стратегических коммуникаций и общей устойчивости общества в понимании кампаний по информационным операциям. Наконец, СМИ играют значительную роль после завершения киберкризиса. События зачастую оцениваются не по тому, как с ними справились с технической точки зрения, а по тому, как их представили обществу. Поэтому НЦКБ планирует серию семинаров для журналистов с целью их ознакомления с техниками и значением стратегических коммуникаций и со способами выявления техник информационной войны. Представителей СМИ постоянно приглашают участвовать в учениях или наблюдать за ними. Зачастую необходимой для разрешения кризиса информацией владеет частный сектор, однако власти все равно не признают его положения за столом.

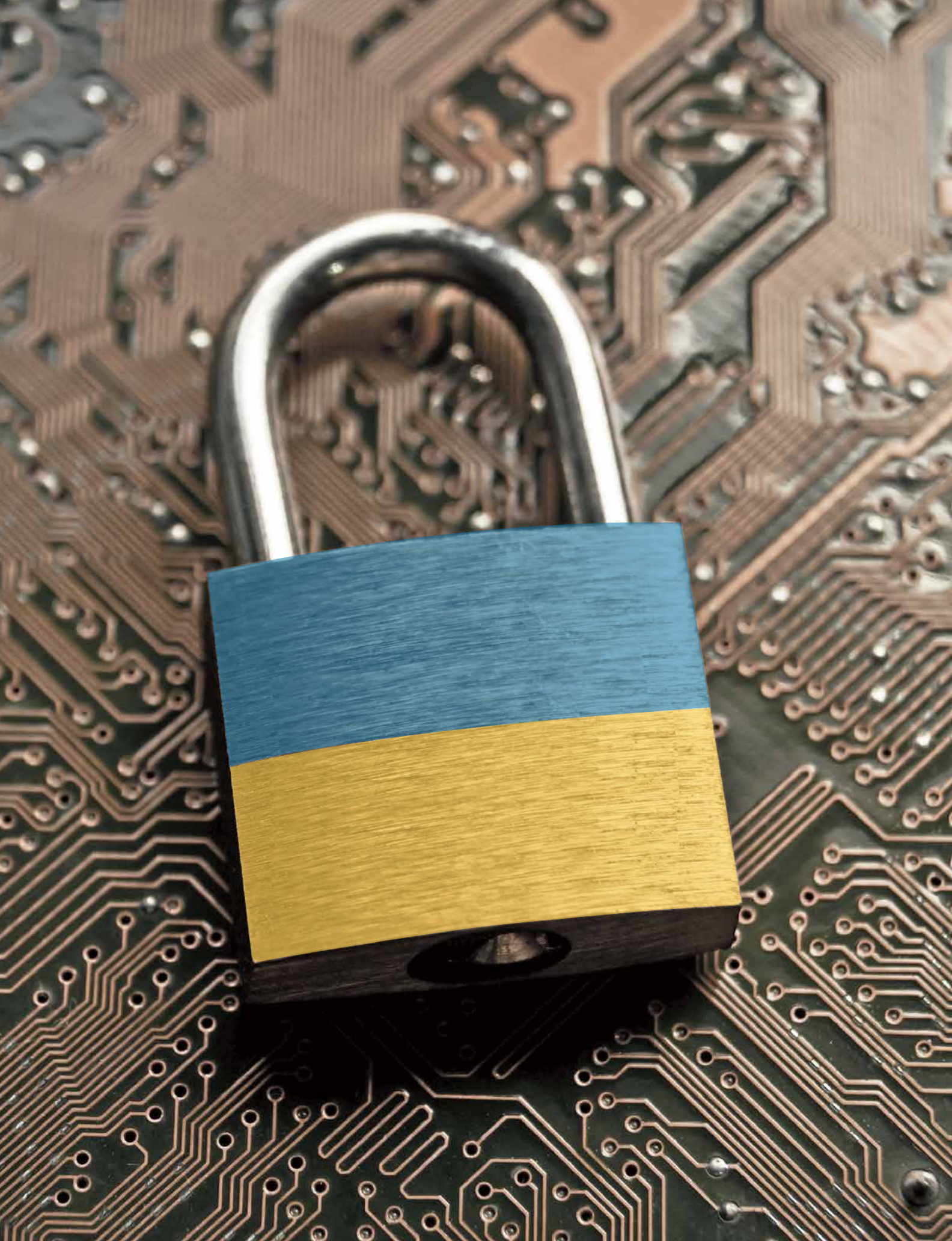
Помимо проведения гибридных учений на национальном уровне, будущее кибербезопасности также заключается в более тесном международном сотрудничестве и в учениях, задействующих разнообразные технические и культурные традиции. Эти цели могут быть достигнуты при помощи расширения международного сотрудничества между государствами, научным сообществом и частным сектором. В Чешской Республике существует упомянутый выше «киберполигон», имеющий научное происхождение и основанный на исследованиях и сотрудничестве в области безопасности с Управлением национальной безопасности. Еще одной ареной проведения киберучений является частный «Кибертренажерный зал» – европейский филиал израильской компании «Cyber Gym». Соединение этих двух полигонов проведения киберучений с аналогичными объектами по всему миру значительно повысит возможности проведения совместных учений с командами, которые – несмотря на универсальность языка информационных и коммуникационных технологий – обладают различными культурными подходами к решению проблем, а также потенциалами, направленными на защиту от различных угроз.

Объединение частных, правительственных и научных учреждений в рамках глобальных учений по кибербезопасности может и не являться новой идеей; однако включение как технической, так и командно-штабной частей, а также использование киберарен, расположенных по всему континенту, на самом деле являются новшествами. Такие учения могут наилучшим образом симулировать будущие конфликты между государственными и негосударственными игроками.

Расширение сферы учений и включение в них сценариев, основанных на недавних событиях, полезны, но более недостаточны. Учения, использующие в качестве модели прошлые инциденты, хороши для повышения ситуационной осведомленности участников. Однако для того, чтобы наилучшим образом использовать преимущества учений по кибербезопасности, критически важно предвидеть неожиданные ситуации и готовиться к ним. Поэтому в рамках рабочей группы по планированию учений НЦКБ создает гибкую структуру под названием «красная клетка». Ее целью является улучшение предвидения возможных тенденций и инцидентов и разработка событий, маловероятных в рамках обычных структур планирования. Другой крайне важной задачей является включение разведывательных служб в технические учения. Поэтому НЦКБ стремится облегчить удаленное участие в учениях, учитывая секретный характер деятельности своих клиентов.

ЗАКЛЮЧЕНИЕ

Если лица, определяющие политический курс, получают понимание различных аспектов киберпространства в результате участия в учениях и таким образом овладевают техническими основами, они могут лучше решать задачу определения политического курса. При помощи учений по кибербезопасности сокращается разрыв между миром политики и техническим миром, а результаты политического планирования привязываются к техническим возможностям. Участие высшего руководства в принятии решений во время учений приводит к лучшим решениям во время кризисов. Обретя в ходе учений более глубокое понимание киберсферы, они не воспринимают ее как нечто относящееся исключительно к IT-сфере и совершенно не поддающееся пониманию. При подготовке комплексных учений НЦКБ стремится включить в них все уровни взаимодействия: оперативный, тактический и стратегический. □



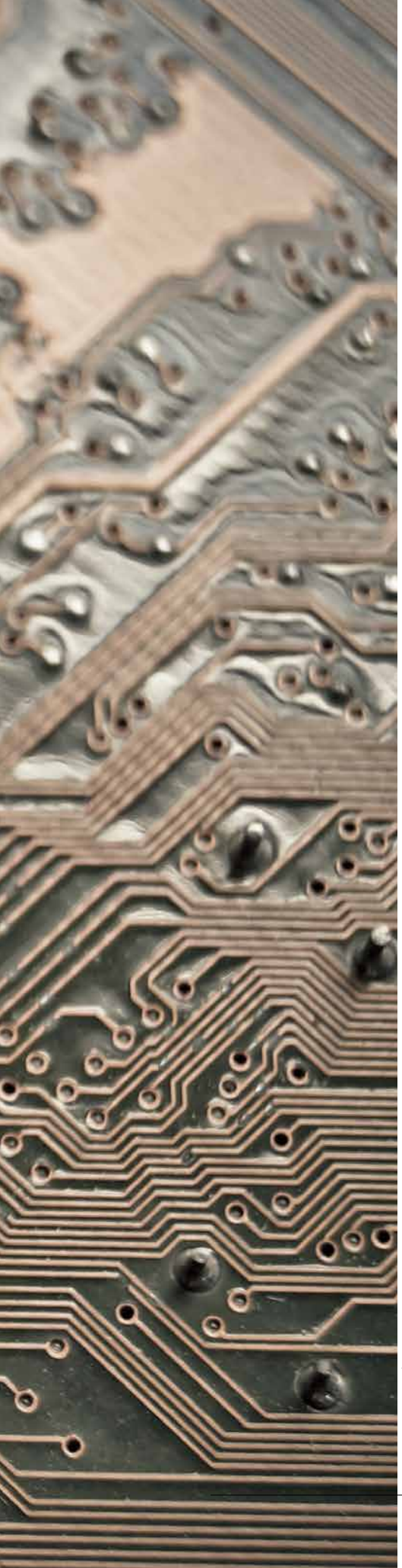


ИЛЛЮСТРАЦИЯ PER CONCORDIAM

ПРОТИВОДЕЙСТВИЕ *КИБЕРУГРОЗАМ* НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УКРАИНА ЗАЩИЩАЕТ СВОЮ КИБЕРИНФРАСТРУКТУРУ НА ФОНЕ АТАК ИЗ РОССИИ

Наталья Ткачук

Быстрое развитие информационных и коммуникационных технологий на Украине, зависимость всех сфер жизни от киберпространства, а также рост киберпреступности и киберагрессии в рамках гибридной войны, которую ведет Россия против Украины – все это доказывает, что кибербезопасность является неотъемлемым элементом национальной безопасности.

Кибербезопасность традиционно рассматривалась на Украине в широком смысле как составная часть информационной безопасности. Однако существующие киберугрозы не только подчеркивают насущную потребность в создании эффективного киберпотенциала и систем кибероборонs, но и в значительной мере меняют роль кибербезопасности. В принятой в 2015 г. Стратегии национальной безопасности Украины кибербезопасность наконец признана полноценной и важной составляющей национальной безопасности.

Согласно отчетам украинской Компьютерной группы реагирования на чрезвычайные ситуации, основной целью кибератак остаются государственный сектор (информационные и телекоммуникационные системы государства) и объекты критической инфраструктуры, в основном в энергетическом секторе.

Недавние кибератаки на энергетические объекты в нескольких регионах Украины привели к отключениям электроэнергии. Тысячи человек провели без электричества несколько часов, была парализована работа предприятий. Данные атаки приписываются многими экспертами Российской Федерации и могут считаться первым примером кибервойны или так называемой гибридной войны, так как они сопровождали действующий военный конфликт и нанесли значительный ущерб критической инфраструктуре другой страны.

Другой отличительной чертой киберугроз национальной безопасности Украины является использование кибератак в качестве инструмента информационной войны. Хакеры, предположительно связанные с российскими спецслужбами, атакуют официальные веб-сайты правительства Украины и размещают на них недостоверную информацию и ложные заявления. Целью этой дезинформации является дискредитация авторитета государства и рост социальной напряженности.

За последние годы резко вырос уровень киберпреступности, еще одной угрозы кибербезопасности Украины. С одной стороны, Украина входит в первую пятерку стран мира по выпуску высококвалифицированных специалистов в области информационных технологий (IT), многих из которых приглашают на работу за границу; ежегодно украинские университеты выпускают 16 тыс. профессионалов в области IT. Однако некоторые из этих

специалистов могут стать объектами манипуляций со стороны киберпреступников или международной организованной преступности. Зачастую они даже не знают реальной цели и конечного назначения результатов своей работы.

15 марта 2016 г. Президент Украины Петр Порошенко подписал указ о введении в действие решения Совета национальной безопасности и обороны Украины от 27 января «О стратегии кибербезопасности Украины».

Данная стратегия была принята с учетом стоящих перед Украиной вызовов: агрессивных действий со стороны Российской Федерации и растущего использования киберпространства разведывательными и специальными военными структурами, а также террористами и преступниками.

Целью Стратегии кибербезопасности является создание условий для безопасного функционирования киберпространства в интересах личности, общества и государства. Стратегия предусматривает широкий комплекс мер по обеспечению кибербезопасности Украины. В частности, эти меры включают в себя создание госполитики, направленной на развитие киберпространства и обеспечение его безопасности, достижение совместимости со стандартами Европейского Союза и НАТО, формирование конкурентной среды в сфере электронных коммуникаций и предоставление услуг по киберзащите.

Согласно данному документу, основу национальной системы кибербезопасности составляют Министерство обороны Украины, Государственная служба специальной связи и защиты информации Украины, Служба безопасности Украины, Национальная полиция Украины, Национальный банк Украины, а также разведывательные органы.

Координационным органом в сфере кибербезопасности является подчиняющийся президенту Украины Совет национальной безопасности и обороны Украины, перед которым поставлена задача по созданию в своем составе Национального координационного центра кибербезопасности.

Тем не менее, на пути к построению эффективной системы кибербезопасности, способной защитить страну от возникающих киберугроз, Украину

ожидают трудности, такие как согласование плана действий по реализации Стратегии кибербезопасности Украины в 2016 г., улучшение механизмов координации и межведомственного взаимодействия, развитие основанного на доверии партнерства между государственным и частным секторами, улучшение технических возможностей и образования, повышение информированности о киберугрозах, а также достижение полноправного членства в международных инициативах и сотрудничество в сфере кибербезопасности.

Учитывая транснациональный характер киберугроз, важную роль в укреплении кибербезопасности Украины играет международное сотрудничество с НАТО, Организацией по безопасности и сотрудничеству в Европе (ОБСЕ) и Европейским союзом, а также двустороннее сотрудничество со странами-партнерами.

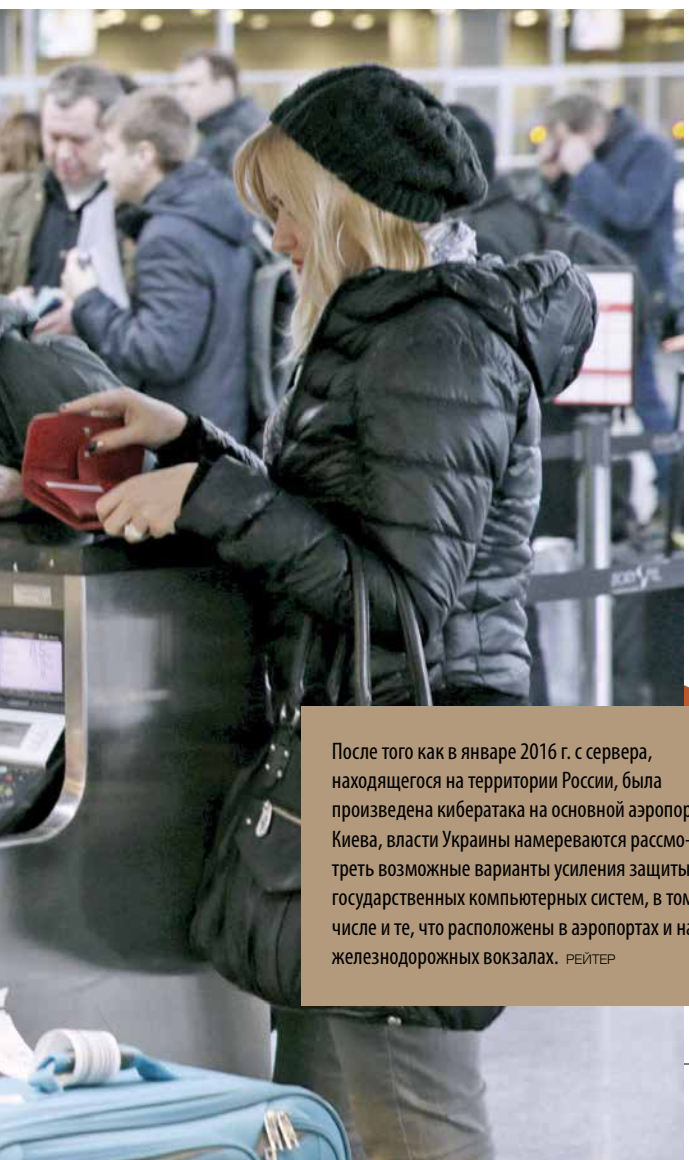
На проходившем в сентябре 2014 г. в Уэльсе саммите НАТО был учрежден Трастовый фонд Украина-НАТО по вопросам кибербезопасности, чьей основной задачей является помощь Украине в развитии технического потенциала противодействия киберугрозам. В рамках данного проекта также осуществляется обучение персонала использованию данных технологий и оборудования и даются практические советы по вопросам выработки политики.

Признавая важность выработки общих международных подходов в вопросах киберпространства и формирования доверия с другими странами в киберпространстве, Украина принимает активное участие в международных инициативах по кибербезопасности. С 2013 г. Украина является активным членом неофициальной рабочей группы в рамках ОБСЕ по мерам укрепления доверия, разработавшей и реализовавшей комплекс мер по снижению рисков конфликтов, проистекающих из использования информационных и коммуникационных технологий.

В 2005 г. Украина ратифицировала Конвенцию Совета Европы о киберпреступности, однако ее отражение в национальном законодательстве все еще продолжается. С точки зрения национальной кибербезопасности, одной из самых срочных задач является реализация положений, наделяющих следственные органы Украины правом издавать обязательные к исполнению правила, предписывающие поставщикам услуг связи незамедлительно сохранять и в дальнейшем хранить компьютерные данные в тех случаях, когда это необходимо для расследования преступлений.

Конвенция о киберпреступности является важным инструментом международного сотрудничества в сфере борьбы с киберпреступностью, однако также существует острая потребность в оптимизации уже существующих механизмов обмена информацией, таких как договор о взаимной правовой помощи, задачей которого является обеспечение быстрого и надлежащего реагирования на киберугрозы и расследования киберпреступлений на национальном и международном уровне.

Сегодня Украина сталкивается с широким спектром разнообразных и изощренных киберугроз, многие из которых являются совершенно новыми. Кибервторжения являются одним из самых серьезных вызовов национальной безопасности. Нельзя гарантировать национальную безопасность Украины, не усилив ее кибербезопасность. Для этого требуется построение и последующее развитие эффективной системы кибербезопасности и комплекса соответствующих мер на основе глобального передового опыта и международной поддержки. Задача состоит не только в противодействии существующим киберугрозам, но и в обеспечении баланса между национальной безопасностью и фундаментальными европейскими ценностями. □



После того как в январе 2016 г. с сервера, находящегося на территории России, была произведена кибератака на основной аэропорт Киева, власти Украины намереваются рассмотреть возможные варианты усиления защиты государственных компьютерных систем, в том числе и те, что расположены в аэропортах и на железнодорожных вокзалах. РЕЙТЕР

ЗАЩИТА
киберпространства *в Грузии*

Для надежной кибероборонны нужны инфраструктура, юридическая поддержка и многонациональное сотрудничество

АНДРИЯ ГОЦИРИДЗЕ, ДИРЕКТОР БЮРО
кибербезопасности Министерства обороны Грузии

Сфера киберпространства растет стремительными темпами, а вместе с ней и уровень и сложность угроз государствам, их информационно-технологическим системам (IT-системам) и соответствующей инфраструктуре. Также возросло количество игроков в киберпространстве, что расширяет спектр методов атаки и количество систем, которые потенциально могут стать их целью. Правительственные информационно-коммуникационные системы, военные и коммерческие проекты становятся более уязвимыми для кибератак и кибершпионажа. В ответ правительства должны создавать более надежные системы кибероборонны.

Для такой страны, как Грузия, находящейся в процессе перехода к цифровой эпохе, эти тенденции представляют серьезную проблему, равно как и возможность кибернападения со стороны ее противников по недавним конфликтам и по геополитической конфронтации.

Здание правительства Грузии в Тбилиси, где правительство страны приняло политику кибербезопасности с акцентом на сотрудничество между государственными, частными и международными организациями. РЕЙТЕР

УГРОЗА

Использование киберэлементов для достижения политических, экономических или военных целей – или для получения геополитического преимущества – является частью современной реальности. Киберпространство Грузии не является исключением. Критическая инфраструктура страны, существующие информационные системы, сети и инфраструктура, принадлежащие другим странам и международным организациям, а также иностранные коммерческие структуры – все они являются возможными целями ввиду членства Грузии в антитеррористической коалиции и взятого ей евроатлантического курса.

Следующие игроки представляют собой потенциальную угрозу:

- страны с высокоразвитым наступательным киберпотенциалом (особенно Россия);
- террористические организации, проводящие кибероперации;
- финансово мотивированные киберпреступники.

Киберпространство превратилось в важный компонент войны и конфликта. Так как Кремль считает, что Грузия находится в его сфере влияния, защита нашего киберпространства должна быть одним из главных приоритетов национальной безопасности. Киберпространство является областью, в которой маленькая страна может противостоять намного более крупному агрессору и применять асимметричные меры реагирования.

ИНФРАСТРУКТУРА КИБЕРБЕЗОПАСНОСТИ

Надежная кибероборона требует крупных вложений, начиная с разработки киберархитектуры и современных стратегических документов и заканчивая интеграцией киберпотенциалов в военные операции. Грузия полностью разделяет позицию НАТО, согласно которой первым шагом на пути к успешному развитию совместной кибербезопасности является построение своего собственного механизма кибероборонны.

Первая для Грузии стратегия и план действий в области кибербезопасности были разработаны в 2013 г. Этот документ на 2013-2015 годы определяет политику правительства страны по кибербезопасности, отражая стратегические задачи и основные принципы, а также устанавливает планы действий. Главной стратегической задачей является сотрудничество между государственными, частными и международными организациями. Стратегия по кибербезопасности включает в себя пять основных элементов: исследование и анализ, нормативно-правовую базу, координацию на институциональном уровне, повышение осведомленности населения при помощи информационно-разъяснительной и образовательной деятельности, а также международное сотрудничество.

В конце 2015 г. по инициативе Совета государственной безопасности и управления кризисами Грузии был разработан План действий по стратегии и развитию в области кибербезопасности на 2016-2018 годы. В нем содержатся новые проекты и меры, необходимые для обеспечения кибербезопасности.

Нормативно-правовая база

Основой нормативно-правовой базы в области кибербезопасности является Закон об информационной безопасности, чьей задачей является поддержка эффективной реализации информационной безопасности, определение обязанности и ответственности государственного и частных секторов и создание механизмов государственного контроля над исполнением политики в области информационной безопасности. Согласно данному закону, Агентство по обмену данными и Бюро кибербезопасности Министерства обороны (МО) Грузии являются ведомствами, ответственными за кибербезопасность страны.

Согласно Уголовному кодексу Грузии, неправомерный доступ к компьютерной информации, создание или распространение вредоносных программ, а также неправомерное использование компьютерных сетей являются преступлениями, равно как и кибертерроризм. На международном уровне в 2012 г. Грузия ратифицировала Конвенцию о киберпреступности, разработанную Советом Европы. Грузия разделяет общие руководящие принципы стран-членов конвенции и намеревается создать всеобъемлющую нормативно-правовую базу на национальном уровне и развивать международное сотрудничество.

Институциональная инфраструктура

Закон Грузии «О порядке планирования и координации политики национальной безопасности» определяет информационную безопасность как составную часть национальной безопасности и устанавливает Совет национальной безопасности и Совет по государственной безопасности и управлению кризисами в качестве органов, отвечающих за планирование политики в области национальной безопасности. Совет национальной безопасности – это президентский консультативный орган, возглавляемый президентом страны, созданный для координирования военного строительства и обороны страны.

После российско-грузинской войны 2008 г. под руководством Совета национальной безопасности был начат процесс пересмотра национальной безопасности. Кибербезопасность была признана в качестве важной составляющей национальной безопасности, а Совет национальной безопасности взял на себя ответственность за координацию кибербезопасности на национальном уровне. Однако после изменения конституции в 2014 г. главой государства стал премьер-министр. При

Совете по государственной безопасности и управлению кризисами при премьер-министре страны был создан консультативный орган, ответственностью которого стала кибербезопасность. Совет осуществляет руководство в сфере информационной безопасности и отвечает за выявление и предотвращение внутренних и внешних угроз, а также координирует разработку национальной стратегии кибербезопасности.

В 2010 г. при Министерстве юстиции было создано Агентство по обмену данными (АОД), задачами которого является разработка стандартов для электронного управления, инфраструктур обмена данными и информационно-коммуникационной сферы Грузии, а также создание и реализация политики в области информационной безопасности. АОД является одним из основных органов, ответственных за разработку и реализацию кибербезопасности. К компетенции Агентства относится обеспечение кибербезопасности всей правительственной сети (за исключением ее военной части), представляющей собой 36 объектов критической инфраструктуры.

Под руководством АОД функционирует Компьютерная группа реагирования на чрезвычайные ситуации (CERT), отвечающая за реагирование на киберинциденты и наблюдение за работоспособностью правительственной сети Грузии. CERT уполномочен требовать доступ к критическим информационным системам или активам. АОД устанавливает минимальные требования по информационной безопасности для критических информационных систем.

Уголовное преследование и расследование киберпреступлений осуществляются Отделом по борьбе с киберпреступностью Центрального отделения криминальной полиции (при Министерстве внутренних дел). В рамках Отдела функционирует круглосуточный контактный центр, осуществляющий обмен информацией о киберпреступлениях с другими членами Конвенции Совета Европы о киберпреступности.

Реализация

В 2014 г. Бюро кибербезопасности приняло политику в области кибербезопасности, определяющую подходы и приоритеты в области кибербезопасности оборонного сектора, его стратегические проблемы, а также достижение эффективного, стабильного и надежного функционирования оборонного сектора. С тех пор Бюро кибербезопасности при МО занимается разработкой эффективных и надежных систем в области информационных и коммуникационных технологий для гражданских подразделений МО и для структурных подразделений Генерального штаба. Компьютерная группа реагирования на чрезвычайные ситуации при Бюро осуществляет наблюдение и защиту критической инфраструктуры и инфраструктуры связи МО от киберугроз и рисков.

На основе указанной политики кибербезопасности был разработан План действий по развитию кибербезопасности, включающий в себя основные задачи бюро на 2016-2018 годы: эффективную разработку кибероборонных потенциалов, повышение осведомленности, межведомственное сотрудничество, создание необходимой нормативно-правовой базы и углубление международного сотрудничества. Основной целью является обеспечение конфиденциальности, подлинности и целостности информации, а также защита прав человека.

СОТРУДНИЧЕСТВО

Анализ недавних конфликтов с участием России демонстрирует вызовы, с которыми столкнется Грузия в процессе развития своих киберпотенциалов. Как сказано выше, основным вызовом является интеграция кибербезопасности в более общие стратегические и практические аспекты как наступательных, так и оборонительных операций. К сожалению, наилучшим примером стратегической интеграции, который может дать НАТО, являются действия России во время украинского кризиса. События на Украине продемонстрировали, что киберэлемент играет ключевую тактическую роль и используется с большей частотой. Недавнее добавление киберпространства в программы военной подготовки, а также участие государственных ведомств в международных учениях являются хорошими предзнаменованиями для развития кибербезопасности в Грузии.

Элементы кибероборонны впервые были включены в учения «Дидгори-2014» и «Дидгори-2015». Наряду с Генштабом Грузии в них участвовали Министерство внутренних дел, Совет по государственной безопасности и управлению кризисами и другие службы.

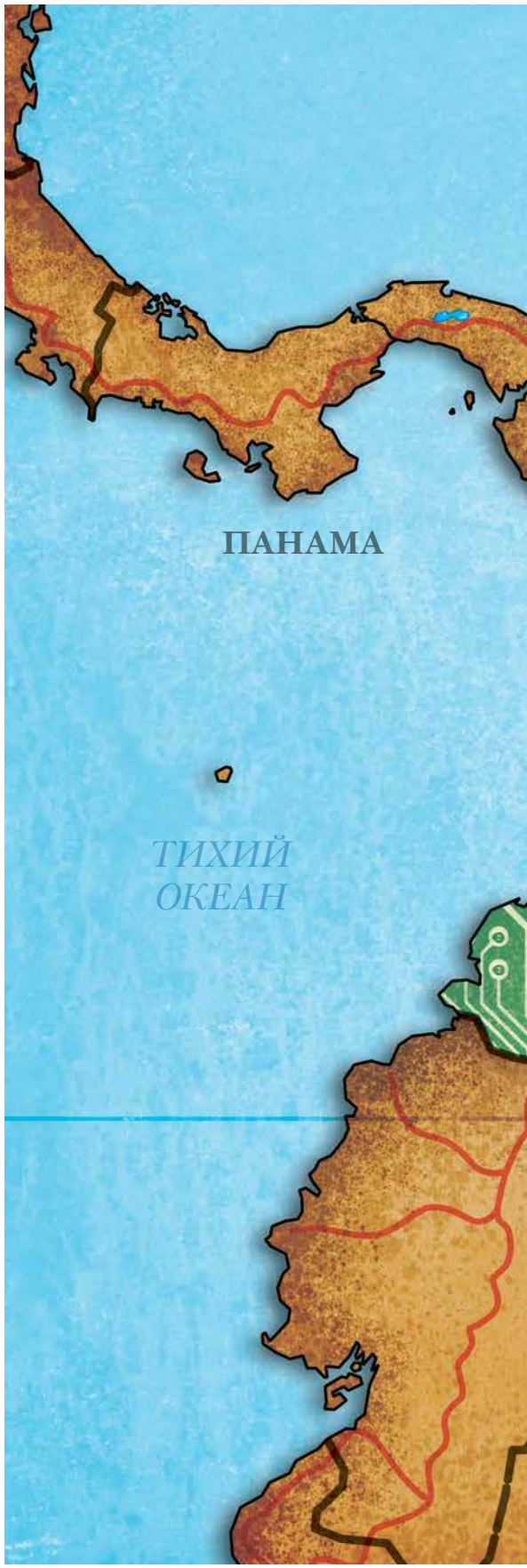
Ценное сотрудничество с Центром передового опыта НАТО в области коллективной кибероборонны и участие в программах «Умной обороны» НАТО имеют чрезвычайно важное значение для развития сферы кибероборонны Грузии, сотрудничества в области обмена информацией и участия в киберучениях «Сомкнутые щиты» и «Киберкоалиция». В 2014 г. представители бюро приняли участие в указанных учениях в качестве наблюдателей. Грузия надеется на укрепление сотрудничества с НАТО с целью полноправного участия в учениях альянса.

Саммит НАТО в Уэльсе в 2014 г. признал фундаментальную важность кибербезопасности для будущего НАТО и для построения единой обороны. Альянс заявил, что совместные кибероперации не только желательны, но и необходимы. Грузия, знакомая с последствиями кибератак и кибершпионажа, признает важность кибербезопасности и разделяет представление НАТО о том, что кибербезопасность – это глобальный вызов, выходящий за рамки национальных границ и требующий сотрудничества на международном уровне. □

КИБЕРБЕЗОПАСНОСТЬ *В* ЮЖНОЙ АМЕРИКЕ

Колумбия разрабатывает новую комплексную политику в области кибербезопасности

Альваро Хосе Чавес Гузман,
Министерство национальной обороны Колумбии



Цифровая экономика и интернет-культура распространяются в странах развивающегося мира ускоренными темпами, и Колумбия находится в авангарде этого процесса. По данным «Доклада о доступности Интернета за 2014 г.», опубликованного Альянсом за доступный Интернет, Колумбия находится на втором месте из 51 развивающейся страны по уровню доступности интернета. Авторы доклада пришли к выводу, что почетным вторым местом Колумбия обязана целому ряду мер со стороны государственных и частных субъектов по осуществлению крупномасштабных инвестиций в инфраструктуру сельских районов страны, а также целенаправленным усилиям по повышению грамотности в области информационно-коммуникационных технологий. Благодаря работе по этим двум направлениям доступ в интернет имеет более половины населения страны.

Усилия Колумбии привели к значительному повышению числа интернет-пользователей: с 2,2 млн. интернет-соединений в 2010 г. до более чем 9,2 млн. в 2014 г. В этом отношении Колумбия стала первой страной в Латинской Америке, обеспечившей высокоскоростным доступом в интернет все муниципальные образования.

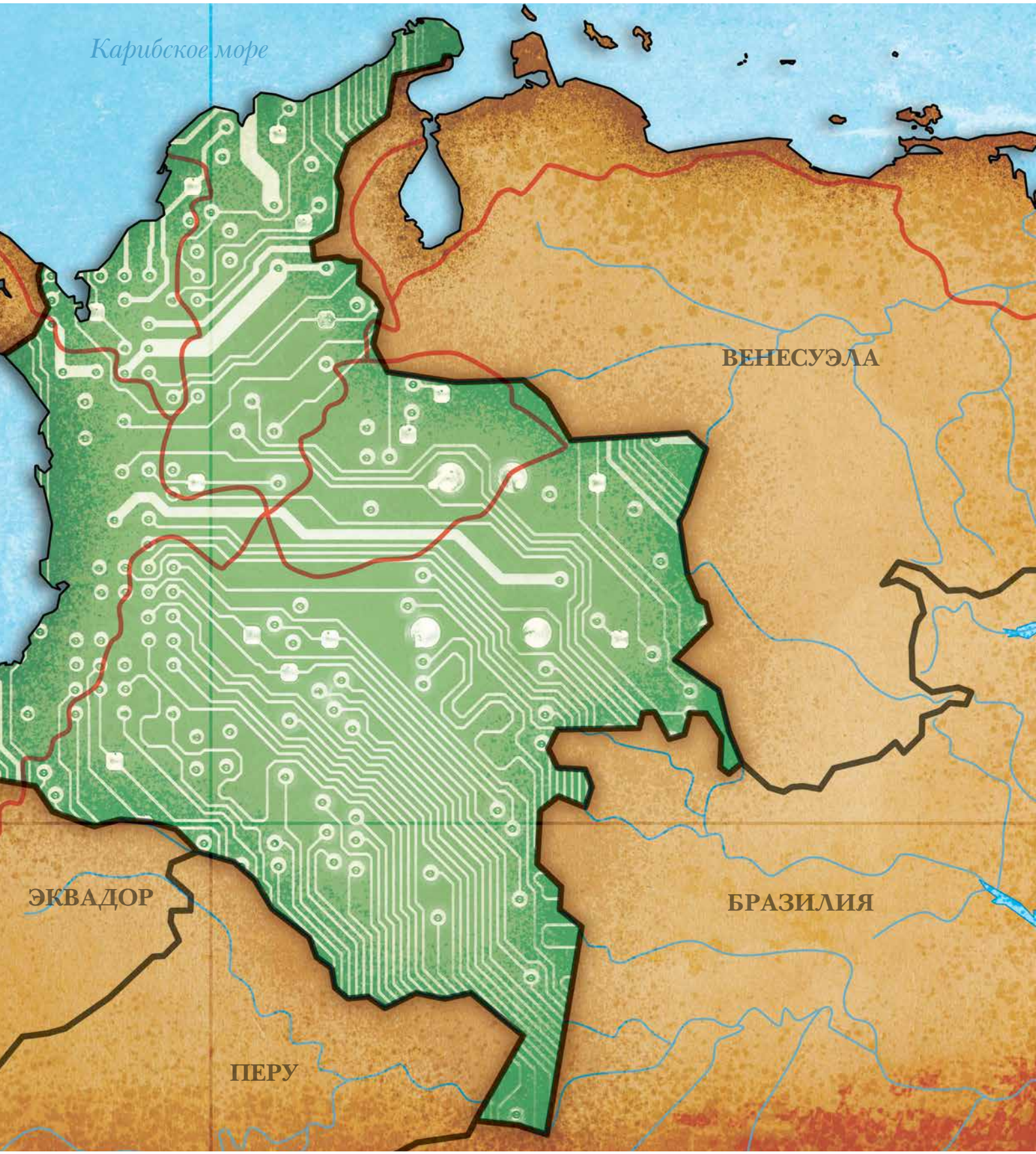


ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

Однако в последние годы интернет все больше используется в преступных целях. С 2007 г. Колумбия разрабатывала национальную стратегию по противодействию киберпреступности с упором на кибероборону и кибербезопасность. Эта стратегия основана на трех основных компонентах:

- Компонент 1: Обеспечить необходимую институциональную базу для мониторинга угроз, предотвращения атак, координирования мер реагирования и выработки рекомендаций по борьбе с угрозами и рисками в киберпространстве.
- Компонент 2: Проводить обучение персонала в области информационной безопасности и расширять исследования в сфере кибероборонь и кибербезопасности.
- Компонент 3: Усилить законодательство, международное сотрудничество и использование международных инструментов по борьбе с киберпреступностью.

Для реализации вышеуказанных стратегий в Колумбии были запланированы и созданы четыре организации:

- Межотраслевая комиссия: определяет стратегическое видение в области управления информацией и устанавливает основные принципы политики в сфере технологической инфраструктуры, открытой информации, а также кибербезопасности и кибероборонь.
- Колумбийская компьютерная команда экстренной готовности (colCERT): координирует национальные аспекты кибероборонь и кибербезопасности.
- Объединенное киберкомандование Главного командования Вооруженных сил: отвечает за защиту от киберугроз, в особенности за защиту критической инфраструктуры страны и оборонного сектора.
- Киберцентр полиции: обеспечивает поддержку и защиту в рамках комплексной политики противодействия киберпреступности.

Данная стратегия преследует три цели:

- Повышает охват и технические возможности путем создания специализированных подразделений.
- Обеспечивает активное участие заинтересованных сторон в реализации стратегии через исполнение ими руководящих функций, разъясняет стратегию частному сектору, повышает образованность граждан и улучшает меры предотвращения на всех уровнях путем использования социальных сетей и иных каналов.
- Пресекает деятельность криминальных структур посредством всеобъемлющего анализа преступлений, расследует функционирование экономики киберпреступности и препятствует ему путем установления связей между полицией страны и различными международными программами; все это в рамках национального программного документа, определяющего руководящие принципы кибербезопасности и кибероборонь.

Несомненно, цели экономического и социального процветания Колумбии носят фундаментальный характер, а решение задачи по обеспечению безопасности и защиты национального киберпространства необходимо для их достижения.

Реализация Национальной стратегии Колумбии по противодействию киберпреступности осуществлялась через Министерство национальной обороны. Хотя эти усилия предпринимаются с учетом важности данного вопроса на международном уровне, также важно, чтобы правительство страны укрепило свою руководящую роль и создало новое и четкое видение интегрированного подхода, учитывающего передовой международный опыт противодействия рискам в киберпространстве.

Доступность интернета в Колумбии резко возросла, что подчеркивает важность надлежащей кибербезопасности. AFP/GETTYIMAGES

На сегодняшний день прогресс в области компьютерных сетей привел к потребности в создании безопасной и надежной цифровой среды для всего общества. И хотя перед созданными Министерством национальной обороны институтами и службами поставлена задача по защите от кибератак и киберпреступности и реагированию на них, необходимо подключить больше заинтересованных сторон из числа властей страны, частных организаций и гражданского общества к согласованным действиям по снижению рисков, проистекающих из опасного поведения или недостаточной информированности о необходимых мерах безопасности.

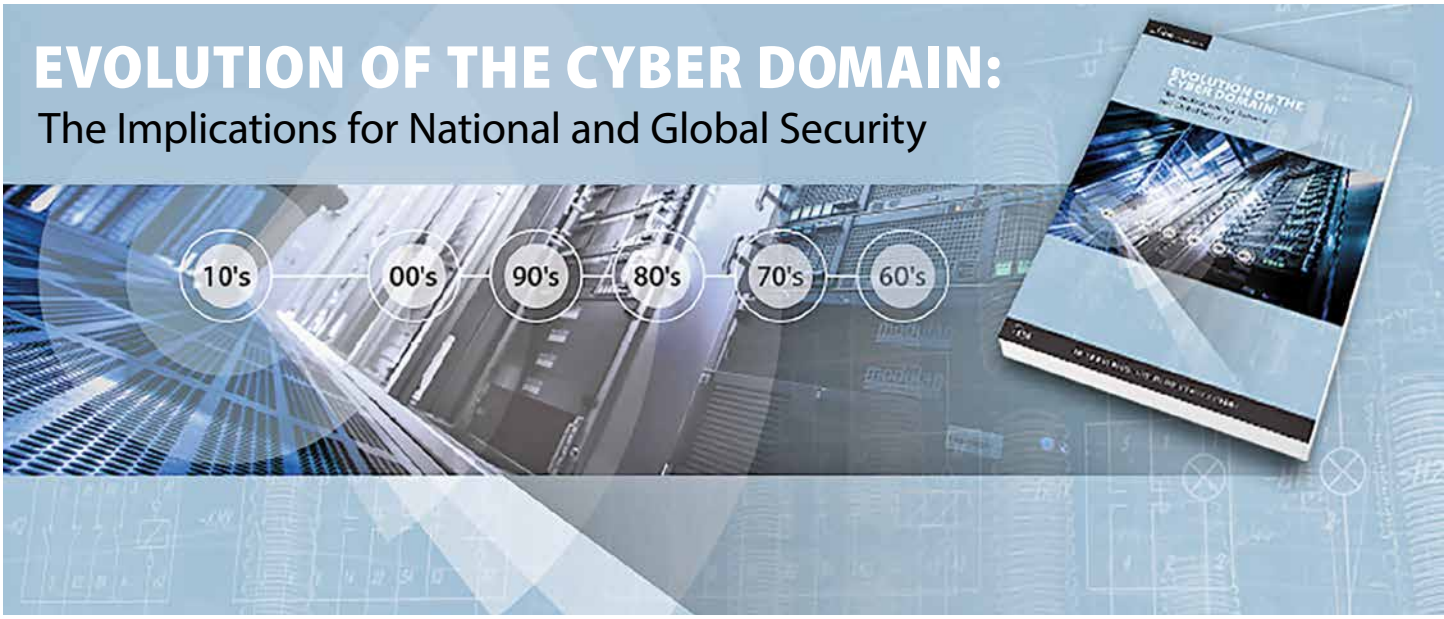
Задача этого нового программного документа заключается в приведении цели в области кибероборонs и кибербезопасности в соответствие с современными реалиями и озвучивании уже созданных потенциалов. Его разработка поддерживалась на высоком правительственном уровне при эффективном и всеобъемлющем участии во всех институциональных моделях со стороны каждого заинтересованного игрока, а именно властей страны, государственных и частных организаций и гражданского общества. Целями, заложенными в данном программном документе, являются экономическое и социальное процветание страны, а его задачами являются создание действенной кибероборонs, борьба с киберпреступностью в цифровой среде и реализация набора фундаментальных принципов, на основе которых можно проводить конкретные мероприятия в рамках управления стратегическими рисками в области цифровой безопасности.

Несомненно, цели экономического и социального процветания Колумбии носят фундаментальный характер, а решение задачи по обеспечению безопасности и защиты национального киберпространства необходимо для их достижения. Вот почему этот новый программный документ в области киберполитики должен стать основой национальной стратегии, которая сможет вывести киберпотенциал Колумбии на новый уровень. Мы можем создать среду, которая будет эффективно способствовать экономическому и социальному процветанию страны; для этого нужно должным образом признать конституционные права и свободы в виртуальном мире и сосредоточить усилия на управлении рисками, на защите критической киберинфраструктуры и национальных интересов в киберпространстве, а также на защите персональных данных и частной жизни граждан. □

История КИБЕРПРОСТРАНСТВА

РЕДАКТОР: Энекен Тик-Рингас, издательство Международного института стратегических исследований, Лондон; ISBN-13: 978-1138654501; декабрь 2015 г.

РЕЦЕНЗЕНТ: Джозеф В. Ванн, Центр им. Маршалла



КНИГА «ЭВОЛЮЦИЯ КИБЕРПРОСТРАНСТВА. ЕЕ ЗНАЧЕНИЕ ДЛЯ НАЦИОНАЛЬНОЙ И ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ» – это редкий сборник, объясняющий, как возникло киберпространство. Привлекательность этой книги основывается на мастерстве, с которым редакторы и авторы берут техническую тему и рассказывают о ней в превосходном повествовательном стиле. В книге подробно излагается последовательность событий, которые в своей совокупности информируют читателя, напоминают ему и просвещают его относительно того, что легко принять как само собой разумеющееся, – об эволюции киберпространства.

На первый взгляд книгу можно ошибочно счесть техническим изданием. Однако каждый абзац полон информации, а благодаря структуре и стилю книги повествование продвигается вперед так, как если бы это был технический триллер, а не энциклопедическая публикация.

Для профессионалов в области стратегии и политики кибербезопасности эта книга обязательна к прочтению и должна занять место в их личных профессиональных библиотеках. Книга снабжена отличным справочным аппаратом, упрощающим дальнейшие исследования и понимание. Более того, отдельные главы могут быть использованы в качестве самостоятельных документов, способных просветить читателей, не имеющих времени или желания читать всю книгу.

Главы книги расположены в грамотном порядке и содержат логичное и понятное описание развития киберпространства. Расположенный на первых страницах книги словарь терминов нарушает традиции и умело связывает расположенные в алфавитном порядке термины с конкретными главами. Этот подход помогает читателю лучше понять терминологию, характерную для эволюции киберпространства. Данная книга представляет интерес как для неспециалиста, так и для эксперта. Для первого она является прекрасным введением в неизвестную область, для второго – содержит описание всех исторических и технических событий, давших начало киберпространству.

Нельзя обойти вниманием вторую часть названия книги, ибо она также играет центральную роль

в ее сюжете. Рассуждения о последствиях для национальной и глобальной безопасности мастерски вплетены в ткань повествования. Читателю напоминают о геополитической ситуации 1950-х и 1960-х годов и о том, как технологический сюрприз в виде запуска Советским Союзом «Спутника-1» заставил администрацию Эйзенхауэра принять решительные меры в ответ на опасения, что США отстают от Советского Союза в области науки и технологии. Эта история помогает понять, почему киберпространству была предначертано играть важную роль в национальной и глобальной безопасности еще до того, как это стало очевидно его изобретателям и пользователям.

В то время как большинству известна роль, сыгранная Агентством по перспективным научно-исследовательским разработкам (ARPA) Министерства обороны США в развитии Компьютерной сети Агентства по перспективным научно-исследовательским разработкам (ARPANET'а), книга раскрывает роль ARPA в более широком контексте оборонно-промышленного комплекса и его роль в разработке технологий обмена компьютерной информацией для решения военных задач. Авторы хорошо показывают, как многие из идей и понятий, легших в основу ARPANET'а, параллельно зарождались и в других местах. Они также объясняют, как США выявили настоятельную потребность в разработке более надежных сетей командования и управления для снижения уязвимости ранних ракетных систем командования и управления. Данный кусочек повествования помогает читателю лучше понять, как много не связанных с ARPA людей и организаций приняли участие в эволюции киберпространства и ее технологическом воздействии на национальную безопасность.

При том, что число не входящих в ARPA участников было достаточно велико, именно Пентагон выделил деньги на покупку дорогого по тем временам оборудования и предоставил его в распоряжение лучших умов. Создание эффективных линий связи между различными компьютерами способствовало объединению ресурсов и ускорило дальнейший обмен идеями. Потенциал APRANET'а, зародившегося в качестве смелого проекта Агентства по перспективным научно-исследовательским разработкам по улучшению американских систем оперативного командования и управления, получил быстрое признание. Давая читателю понять логику, действовавшую в контексте проблем времен Холодной войны, авторы помещают сюжет в контекст задач, доминировавших в принятии решений на государственном уровне. В книге подчеркиваются причины, по которым США и, в меньшей степени, другие западные страны понимали экономическое значение развития киберпространства и намеренно ограничивали получение Советским Союзом информации о нем и о связанных с ним технологиях из-за опасений, что коммунисты будут использовать их в военных целях.

В последующих главах книга проводит читателя через историю научно-технических разработок в киберсфере, подчеркивая новые открытия и решения проблем в области технологий, а также фокусируясь на важности киберпространства для национальной безопасности. Когда военный сегмент ARPANET'а был отделен от гражданского, последний получил возможность установить связи с учеными по всему миру. Это создало потребность в технологиях, которые могли бы удовлетворять возрастающие требования к возможностям сетевого взаимодействия. Именно сетевое взаимодействие оказалось ключевым фактором, стимулировавшим развитие новых технологий и еще больше увеличившим технологический разрыв со странами Восточного блока.

Книга систематически знакомит читателя с новыми разработками в области технологии и программного обеспечения и с тем, как каждое из них влекло за собой инновации, сыгравшие свою роль в более широкой эволюции киберпространства. Рассказывая об эволюции кибертехнологий в 1970-1990-е годы, авторы рисуют четкую картину того, как и почему на эволюцию киберпространства оказали влияние его растущие коммерческие приложения, приведшие к возникновению новых пользователей и, в свою очередь, к потребностям в новых технологиях.

Растущая сложность аппаратного и программного обеспечения привела к необходимости в управлении интернетом. Авторы заостряют внимание на эволюции различных правительственных форумов, а также на вызовах и соображениях в области управления сетевым взаимодействием. Это дает четкое понимание того, как развивалось управление интернетом, и почему ограниченное «правительственное» вмешательство в интернет, возможно, на самом деле является причиной его грандиозной полезности и роста.

Заключительные главы рисуют четкую и на удивление современную картину важности кибербезопасности и ценности той роли, которое киберпространство играет в поддержке разведывательного сообщества. Хотя книга тщательно обходит стороной споры о роли киберпространства в революции в военных вопросах, читатели не могут не прийти к своим собственным выводам о ключевой роли, которую оно играет в современной военной и национальной безопасности.

Эта исключительная книга заслуживает широкой популярности среди интересующихся киберсферой читателей, однако ее главным недостатком является цена. Книга стоит 90 фунтов стерлингов, или около 128 долл. США, и эта высокая цена, скорее всего, ограничит ее доступность и лишит книгу широкого круга читателей, которого она достойна. □

Стационарные курсы

Democratia per fidem et concordiam
Демократия через доверие и дружбу

Отдел регистрации
George C. Marshall European Center for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany

Телефон: +49-8821-750-2327/2229/2568
Факс: +49-8821-750-2650

www.marshallcenter.org
registrar@marshallcenter.org

Порядок регистрации
Европейский центр исследований по вопросам безопасности имени Джорджа К. Маршалла не принимает заявлений напрямую. Заявления на все курсы должны поступать через соответствующее министерство и посольства США или ФРГ в стране проживания кандидата. Тем не менее, отдел регистрации слушателей готов помочь кандидатам в проведении процедуры. Запрос можно направить по электронному адресу: registrar@marshallcenter.org

ПРОГРАММА ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ (ПАСС)

Основной курс очного обучения Центра Маршалла рассчитан на 8 недель и охватывает такие сферы, как политика безопасности, вопросы обороны, международные отношения, включая международное право и борьбу с терроризмом. Основной темой, рассматриваемой на протяжении всей программы, является необходимость международного, межведомственного и междисциплинарного сотрудничества.

ПАСС 16-15
22 Сентября -
17 Ноября 2016

Сентябрь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Октябрь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Ноябрь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

ПРОГРАММА «БОРЬБА С ТРАНСНАЦИОНАЛЬНОЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ» (БТОП)

Двухнедельный очный курс, посвященный таким угрозам национальной безопасности, как незаконный оборот и прочие виды преступной деятельности. Курс адресован государственным и правительственным служащим и специалистам-практикам, участвующим в разработке политики, реализации правоохранительных, разведывательных мероприятий и контрмер.

БТОП 17-01
30 Ноябрь -
15 Декабрь 2016

Ноябрь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Декабрь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

БТОП 17-09
10-25 Май 2017

Май

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

ПРОГРАММА «ТЕРРОРИЗМ И ВОПРОСЫ БЕЗОПАСНОСТИ» (ПТВБ)

Эта четырехнедельная программа рассчитана на государственных служащих и офицеров вооруженных сил, которые в настоящее время работают на среднем и высшем уровнях управления организаций по борьбе с терроризмом, и она содержит сведения о характере и масштабах современной террористической угрозы. Программа повысит способность слушателей бороться с последствиями терроризма на региональном уровне за счет предоставления основных знаний, которые позволят служащим органов национальной безопасности сотрудничать на международном уровне в деле борьбы с террористической угрозой.

ПТВБ 17-05
02-30 Март 2017

Март

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

ПТВБ 17-13
06 Июль -
03 Август 2017

Июль

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Август

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

ПРОГРАММА ПО ИЗУЧЕНИЮ ВОПРОСОВ КИБЕРБЕЗОПАСНОСТИ (ПВКБ)

Курс посвящен тому, как решать проблемы киберпространства в соответствии с основополагающими ценностями демократического общества. Это нетехническая программа, которая помогает участникам понять характер и масштабы современных угроз.

ПВКБ 17-04
31 Январь -
16 Февраль 2017

Январь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Февраль

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28				

СЕМИНАР ПО РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ (СРБ)

Семинар продолжительностью три недели имеет целью систематический анализ характера отдельных кризисов, влияния региональных субъектов, а также воздействия международных мер помощи.

СРБ 17-07
04-27 Апрель 2017

Апрель

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

СЕМИНАР ДЛЯ ВЫСШЕГО РУКОВОДЯЩЕГО СОСТАВА (СВРС)

Это интенсивная пятидневная программа, посвященная новым ключевым глобальным тенденциям, которые могут привести к появлению новых точек зрения, концепций и совместных обсуждений, а также возможных решений. Программа предназначена для высшего офицерского состава, дипломатов высокого ранга, послов, министров, заместителей министров и парламентариев. СВРС состоит из официальных презентаций, проводимых высшими должностными лицами и признанными специалистами, с последующим всесторонним обсуждением в семинарских группах.

СВРС 16-9
12-16 Сентябрь 2016

Сентябрь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

СВРС 17-10
05-09 Июнь 2017

Июнь

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

ПРОГРАММЫ ДЛЯ ВЫПУСКНИКОВ

Дин Рид, Директор программ для выпускников
тел +49-(0)8821-750-2112
reeddg@marshallcenter.org

Специалисты по связям с выпускниками

Барбара Уизер
Юго-Восточная Европа

Языки: английский, русский, немецкий, французский

тел + 49-(0)8821-750-2291
witherb@marshallcenter.org

Кристиан Эдер
Западная Европа

Языки: английский, немецкий

тел + 49-(0)8821-750-2814
christian.eder@marshallcenter.org

Марк Джонсон
Центральная Азия, Южный Кавказ, Россия, Молдова, Украина, Беларусь – Специалист по кибервопросам

Языки: английский, русский, французский

тел + 49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Кристофер Бурелли
Центральная Европа, Прибалтийские государства – специалист по противодействию терроризму

Языки: английский, словацкий, итальянский, немецкий

тел + 49-(0)8821-750-2706
christopher.burelli@marshallcenter.org

Донна Джанка
Африка, Ближний Восток, Южная и Юго-Восточная Азия, Северная и Южная Америка – специалист Оперативного центра по противодействию терроризму (СТОС)

Языки: английский, немецкий

тел + 49-(0)8821-750-2689
nadonya.janca@marshallcenter.org

mcalumni@marshallcenter.org

Подать материал для публикации

Вы заинтересованы в подаче материалов для публикации в журнале *per Concordiam*? Правила подачи материалов для публикации можно найти по адресу **http://tinyurl.com/per-concordiam-submissions**

Подписаться

Если Вы хотите подписаться на **БЕСПЛАТНУЮ** доставку журнала *per Concordiam*, пожалуйста, свяжитесь с нами по электронной почте **editor@perconcordiam.org**

Найти нас

Вы можете найти *per Concordiam* на интернете по адресу:
Центр Маршалла: **www.marshallcenter.org**
Twitter: **www.twitter.com/per_concordiam**
Facebook: **www.facebook.com/perconcordiam**
GlobalNET портал: **https://members.marshallcenter.org**
Цифровая версия: **http://perconcordiam.com**

Европейский центр исследований по вопросам безопасности имени Джорджа К. Маршалла в Гармиш-Партенкирхене, Германия.

ФОТОГРАФИЯ ПРЕДОСТАВЛЕНА ЦЕНТРОМ ИМ. МАРШАЛЛА