ТОМ 10, № 4, 2020

# per Concordiam

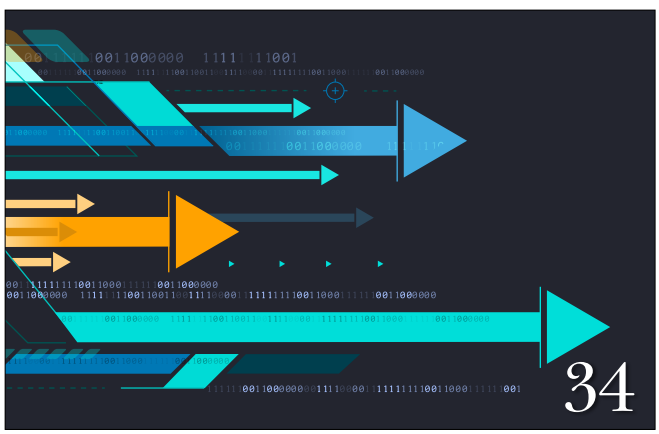
*Журнал по проблемам безопасности и обороны Европы*



## ОСТРАЯ НЕОБХОДИМОСТЬ В РАЗВИТИИ ТРУДОВЫХ РЕСУРСОВ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

# основные статьи



# *разделы*




## *В каждом номере*



## РЕЦЕНЗИЯ НА КНИГУ




*на обложке:*

Найти, обучить и удержать квалифицированных компьютерщиков чрезвычайно важно для национальной безопасности.

*ИЛЛЮСТРАЦИЯ PER CONCORDIAM*

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

*Представляем* вашему вниманию 40-й выпуск журнала *per Concordiam*. Недостаток квалифицированных специалистов является одной из наиболее серьезных проблем в сфере кибербезопасности во многих странах мира. По оценке одного заслуживающего доверия источника, к 2022 г. в мире будет более 1,8 млн. незаполненных вакансий в этой сфере деятельности. Страны все больше полагаются не только на надежную киберзащиту, но также и на кибербезопасность в области торговли, образования, здравоохранения и других ключевых сферах современной жизни. Это означает, что сегодняшняя нехватка кадров в сфере кибербезопасности завтра обернется проблемами в сфере национальной безопасности.

Соединенные Штаты разрабатывают рекомендации по развитию национальных трудовых ресурсов, расширяя усилия Национального института стандартов и технологий (NIST) при Министерстве торговли США и приобретая все большее количество международных партнеров. В наше время, когда правительство подвергается жесткой критике, Национальная образовательная инициатива (NICE) в рамках NIST является ярким примером того, как правительство может консолидировать разноплановые транснациональные сети и активизировать их деятельность для достижения позитивных перемен. Структура NICE создавалась как гибкая система для всех групп правительственных кругов и гражданского общества, предназначенная для использования при разработке стратегий в сфере обучения и подготовки трудовых резервов в области кибербезопасности.

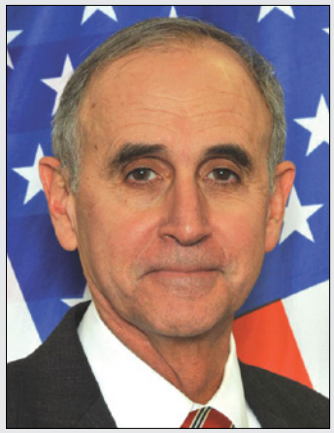
По своей сути, кибербезопасность представляет собой проблему, с которой сталкиваются многие страны. Одни государства находятся в относительно выгодном положении благодаря внедрению образовательных программ и системы национальных приоритетов, в то время как другие, создающие профессиональные кадры в сфере кибербезопасности с нуля, вынуждены приглашать квалифицированных специалистов из других стран. В этом выпуске журнала *per Concordiam* представлены различные точки зрения на эту мировую проблему. Как и в случае с другими вызовами в сфере кибербезопасности, при создании необходимых трудовых ресурсов наилучшим решением являются партнерские отношения, когда гражданское общество, академические круги, частные компании и правительственные ведомства работают сообща. Если смотреть на проблему с позиции государственных учреждений, на первый взгляд может показаться, что в кадровом вопросе частные компании будут представлять непреодолимую проблему, поскольку они могут предложить работникам более щедрое вознаграждение, чем правительственные учреждения. В том, что касается набора персонала, правительство начинает понимать, что его сильной стороной является относительная стабильность рабочего места и инвестиции в работников в целях их удержания. Обучение, удовлетворенность в течение длительного времени и возможность работать на благо своей страны – вот только несколько факторов, которые должны стать приоритетными для правительства, пытающегося преодолеть нехватку специалистов в сфере кибербезопасности.

Очный курс Программы изучению кибербезопасности (ПВКБ) в Центре им. Маршалла расширяет диалог и обучение в сфере подготовки кадров по информационным технологиям по многим направлениям. Помимо вопросов, связанных с подготовкой квалифицированных кадров для этой сферы, курс также рассматривает в отдельных модулях такие аспекты как разработка стратегии в области кибербезопасности, информированность населения об этой проблеме, общегосударственный подход к решению проблемы, варианты сертификации, а также стандарты и рекомендации. Потребность в образовательных программах по информационным технологиям возрастает с каждым годом. Я призываю вас ознакомиться с рекомендациями, которые дают авторы публикаций в этом выпуске. Вы играете ключевую роль в укреплении кибербезопасности в своей организации и за ее пределами. Так приступайте к решительным действиям!

Мы приглашаем вас поделиться своими комментариями и соображениями на эту тему. Пожалуйста, связывайтесь с нами по адресу editor@perconcordiam.org

Искренне ваш,

Кит В. Дейтон
Директор

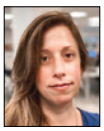


**Кит В. Дейтон**
***Директор***
*Европейского центра по изучению вопросов безопасности им. Дж. К. Маршалла*

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.

**Изабель Баптиста –** координатор Отдела развития и инноваций Национального центра кибербезопасности Португалии. У нее степень магистра по предмету «Право информационной безопасности и киберпространства», для получения которой она написала диссертацию на тему человеческого фактора в сфере кибербезопасности. Многие годы она была ИТ-инструктором в государственных школах и в частном секторе. В последние годы ее деятельность в основном была сосредоточена на повышении информированности общества о важности сферы кибербезопасности путем учебных программ для групп населения и организаций.

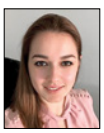
**Руперт Брандмейер** занимал различные управленческие должности в сфере международного бизнеса. У него большой опыт в качестве академического исследователя и лектора по предметам бизнес-администрирования и экономики, кибербезопасности и археологии.



**Мариана Галан –** юрисконсульт Управления киберпреступности Министерства безопасности Аргентины. Ранее она была юрисконсультом по вопросам технологий в Кабинете министров, Министерстве модернизации и Министерстве иностранных дел. С 2016 г. она член Комиссии общественной политики, прав человека и конфиденциальности цифровых операций при Фонде CAPA 8 и отвечает за инициативы привлечения женщин в сферу компьютерных технологий.

**Йорн-Александр Хей –** немецкий офицер-связист (в резерве) с более чем 28-летним опытом, приобретенным в том числе и в ходе международных миссий в Объединенных Арабских Эмиратах и других странах Ближнего Востока. Он работал на должностях старшего главного консультанта, руководителя группы, менеджера проектов и менеджера программ в ходе реализации различных технических и бизнес-проектов в Германии и в других странах.

**Педро Ханисес –** основатель и координатор академической деятельности Фонда CAPA 8. Он также работает в должности советника в Отделе расследований киберпреступлений в Министерстве безопасности Аргентины. Он был национальным директором Управления защиты критически важной информационной инфраструктуры и кибербезопасности, а также директором Национального отдела технологической информации; обе эти должности при Кабинете министров Аргентины. До этого он был руководителем Отдела технологий и безопасности в Министерстве юстиции, безопасности и прав человека и руководителем Отдела технологий и безопасности в Министерстве внутренних дел.



**Клорента Януши –** эксперт по вопросам информационной безопасности в Национальном агентстве электронной сертификации и кибербезопасности при Совете министров Албании. Она член совета директоров организации «Женщины Албании в сфере технологий» и участвовала в организации инициативы «Women4Cyber», нацеленной на расширение участия женщин в работе сектора кибертехнологий.

**Д-р Марко Крстич –** старший советник по вопросам безопасности в Национальной группе реагирования на чрезвычайные компьютерные ситуации Сербии. Он специализируется на тематике использования «обучаемых машин» в сфере кибербезопасности. Он участвует в нескольких международных проектах, относящихся к анализу цифровых криминологических доказательств с применением «разумных систем»; к международному сотрудничеству в таких вопросах как противостояние буллингу, миграция и интеграционные процессы в школах; он также участвует в проекте Casper, пропагандирующем доверие будущих поколений к интернету.

**Геналин Масалинао –** главный специалист по вопросам политики в Бюро кибербезопасности в Отделе информационных и коммуникационных технологий Филиппин. Она является одним из авторов книги «На пути к жизнестойкой региональной кибербезопасности: перспективы и проблемы в Юго-Восточной Азии», вышедшей в 2019 г., а также была в числе главных разработчиков Национального плана Филиппин в сфере кибербезопасности до 2022 г.

**Августин Мальпеде –** юрист в Университете Буенос Айреса, Аргентина, специализирующийся на информационном праве. Он также советник в Фонде CAPA 8 и юрисконсульт в канцелярии помощника министра административных инноваций.

**Д-р Педро Хавьер Мендоса –** консультант в Национальном центре кибербезопасности Португалии, где он координирует работу Наблюдательного центра кибербезопасности и сотрудничает с Программой информированности и обучения. Он также занимается исследовательской и преподавательской работой. Его исследования сосредоточены на социальных аспектах технологий с особым упором на отношения между технологическим развитием средств коммуникации и пользователями. В его последних работах анализируется роль человеческого поведения в сфере кибербезопасности.

per Concordiam

*Журнал по проблемам безопасности и обороны Европы*

РАЗВИТИЕ ТРУДОВЫХ РЕСУРСОВ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Том 10, № 4, 2020



**Центр им. 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* является профессиональным журналом, публикуемым ежеквартально Европейским командованием США и Европейским центром по изучению вопросов безопасности имени Джорджа К. Маршалла, посвященный вопросам обороны и безопасности в Европе и Евразии для учёных и экспертов, занимающихся проблемами обороны и безопасности. Высказанные в журнале взгляды не обязательно отражают политику или точку зрения этих организаций или других государственных ведомств Германии и США. Мнения, высказанные авторами статей, принадлежат исключительно этим авторам. Министр обороны принял решение о том, что публикация этого журнала необходима для поддержания связей с общественностью, как того требует от Министерства обороны США действующее законодательство.

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

**Мадан Кумар Мулхе –** специалист по кибербезопасности в Отделе безопасности информационных технологий Министерства информационных технологий, коммуникаций и инноваций Маврикия. У него более 14 лет опыта работы в сфере информационных и коммуникационных технологий и управления информационной поддержкой, а также более 7 лет работы в руководстве различными проектами и в сфере кибербезопасности. Он сертифицированный «Профессионал в сфере информационных технологий» (2014 г.) и сертифицированный «Ведущий аудитор» (2006 г.) для стандарта информационной безопасности ISO/IEC 27001.

**Вероника Нетолицка –** начальник Отдела национальной стратегии и политики в Управлении правил и процедур кибербезопасности Национального агентства компьютерной и информационной безопасности Чешской Республики. В 2018 г. она работала во Вьетнаме в Технологическом университете им. Хо Ши Мина в качестве исследователя по долгосрочному контракту.

**Петр Новотны –** начальник Отдела киберучений в Управлении правил и процедур кибербезопасности Национального агентства компьютерной и информационной безопасности Чешской Республики. В круг его обязанностей входит обучение сотрудников правительственных учреждений посредством проведения семинаров и учебных курсов.

**Ондрей Ройчик –** руководитель и один из основателей Отдела стратегической информации и анализа Национального агентства компьютерной и информационной безопасности Чехии. У него более 14 лет стажа работы в качестве аналитика проблем международной безопасности, включая работу в Министерстве внутренних дел Чехии и в НАТО. У него степень магистра в вопросах безопасности от Университетского колледжа в Лондоне и докторская степень в международных отношения от Университета им. Масарика в г. Брно в Чешской Республике.

**Д-р Флориан Рупп** участвует в проектах, связанных с компьютерными и цифровыми технологиями, в качестве директора «мозгового треста» «Cyber & Innovation Labs», в качестве главного специалиста по цифровым технологиям компании «RailMaint GmbH», и в качестве старшего руководителя проектов и главного консультанта компании «BWI GmbH». Он также является научным сотрудником Исследовательского центра кибероборонны Университета Вооруженных сил Германии и Технического университета в Мюнхене.

**Даниела Сантос –** аспирантка, изучающая общественную политику и вопросы кибербезопасности. Она член Дискуссионной группы по вопросам жизнестойкости киберпространства в Национальном институте обороны. С 2018 г. она работает в должности руководителя проекта «Информированность и обучение» в португальском Национальном центре кибербезопасности.

**Даниэль Сантос –** менеджер программ Национальной образовательной инициативы в сфере кибербезопасности (NICE) в Национальном институте стандартов и технологий, где она руководит административными, организационными и коммуникационными направлениями работы программного офиса NICE, а также его стратегией международного сотрудничества. Она также работает в должности руководителя программ формального обучения в сфере кибербезопасности, в том числе и в Национальных центрах академического мастерства, а также в Киберкорпусе и отделе стипендий за службу в Министерстве внутренней безопасности США.

**Д-р Лино Сантос –** руководитель португальского Национального центра кибербезопасности и назначенный член совета директоров Европейского агентства по кибербезопасности. Ранее он был директором Службы безопасности и пользователей в Национальном фаонде научной информатики. У него имеются сертификаты в управлении группами реагирования на инциденты в сфере кибербезопасности от Университета Карнеги Меллон и от Программы исследований проблем кибербезопасности Центра им. Маршалла.

**Максимилиано Скаримболо –** начальник управления полиции г. Буенос Айрес. Он уже 22 года занимается расследованием и предотвращением сложных преступлений и защитой высокопоставленных лиц. Он также участвует в работе Фонда CAPA 8. Он преподает курсы по различным специальностям, относящимся к правоохранительной деятельности.

**Д-р Максимилиан Шуберт –** генеральный секретарь австрийской Ассоциации интернет-провайдеров (ISPA). Он специализируется на вопросах юридической ответственности интернет-провайдеров, телекоммуникационном наблюдении и обеспечении соблюдения законности в интернет-среде. Он является президентом EuroISPA, крупнейшей в мире ассоциации интернет-провайдеров, в которой он также занимает должность председателя Комитета по кибербезопасности.

**Ацуко Секигучи –** заместитель советника Международной стратегической группы в Национальном центре готовности к инцидентам и стратегии кибербезопасности (NICS) при секретариате кабинета министров Японии. В круг ее обязанностей входит координация национальной политики в сфере кибербезопасности и организация международного сотрудничества в сфере киберпространства.

**Рэки Сей –** инженер-электронщик, специалист по телекоммуникациям, начальник Управления безопасности информационных систем и цифрового доверия в Министерстве цифровой экономики и телекоммуникаций Сенегала. Она член Исследовательской группы 17 (вопросы безопасности) в Бюро стандартизации Международного союза электросвязи. Она также участвует в работе Глобального форума по киберзнаниям.

**Д-р Вилма Томцо –** генеральный директор Национального агентства по электронной сертификации и кибербезопасности при Совете министров Республики Албания. У нее докторская степень в области информационных систем, и она проработала 24 года в секторе телекоммуникаций. С 2013 г. по 2017 г. она работала в канцелярии премьер-министра на должности директора Европейского управления развития информационных и коммуникационных технологий. Управление принимало участие в разработке цифровых и инновационных правил и процедур, общественных административных реформ, реализации национальных задач в киберпространстве и совершенствовании системы государственных услуг.

**Елика Вуядинович –** советник по вопросам безопасности Национальной группы реагирования на чрезвычайные компьютерные ситуации Сербии. Она занимается урегулированием на национальном уровне инцидентов в сфере кибербезопасности, анализирует уязвимые места и риски с тем, чтобы повысить уровень информированности общества, а также проводит обучение всех заинтересованных сторон в сфере кибербезопасности. Она принимает участие в разработке правил и процедур в Республике Сербия, относящихся к сфере кибербезопасности.

**Клеменс Войвод** имеет 24 года международного опыта в качестве исследователя и преподавателя в области теоретической химии и биологии. У него есть опыт в создании и применении научных компьютерных программ, а также подготовка в области системного администрирования и высококачественной информатики и опыт административного руководства научными проектами. Он занимался исследовательской работой в Германии, Норвегии и Соединенных Штатах.

*Кадры в сфере кибербезопасности*

# В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ НАЦИОНАЛЬНОЙ ОБОРОНЫ

**Том Уингфилд**, Министерство обороны США

Однажды Альберта Эйнштейна, известного ученого, родившегося в Германии, спросили, как бы он распорядился одним часом времени, который бы ему дали на то, чтобы спасти мир. На мгновение задумавшись, он ответил, что первые пятьдесят пять минут он потратил бы на то, чтобы определить суть проблемы, а за оставшиеся пять минут решил бы ее.

Сегодня мы пытаемся определить, как сделать так, чтобы самая главная составляющая кибернетической экосистемы – человеческий компонент – была готова к планированию, созданию, обслуживанию, использованию и защите нашей компьютерной инфраструктуры. Нехватка опытных аналитиков и работников в сфере кибербезопасности, несмотря на очевидный спрос на них, по-прежнему остается глобальной проблемой как для частного сектора, так и для государственного, что хорошо отражено в соответствующих документах. Конечно, не все, но большинство руководителей государственных органов и ведущих компаний отрасли осознают потребность в более высоком уровне безопасности и жизнестойкости киберпространства и пытаются что-то предпринять в этом направлении.

Признавая, что трудовых ресурсов в сфере кибербезопасности недостаточно, и что распределены они неравномерно, даже в секторе национальной безопасности США, президент Трамп в мае 2019 г. издал указ, направленный на стимулирование роста числа этих специалистов в органах федерального правительства. «Наша нация испытывает нехватку одаренных и способных специалистов в сфере кибербезопасности, и поэтому требуются новаторские подходы к повышению доступности обучения, которое поднимет профессионалов в этой области на максимально высокий уровень знаний, навыков и способностей», - написал президент. Развивая эту идею, в недавно опубликованном «Отчете-справке» созданной Конгрессом двухпартийной Комиссии по киберпространству (Cyberspace Solarium Commission) указывается, что «Конгресс и исполнительная власть должны принять законы и ввести правила, позволяющие более эффективно нанимать, обучать и удерживать одаренных специалистов, одновременно с этим увеличивая число кандидатов на вакансии по кибернетическим специальностям в федеральном правительстве».

В ответ на такое поручение Министерство обороны США (МО) со штатом 1,4 млн. человек на действительной службе, 1,1 млн. резервистов и 861 тыс. гражданских служащих на территории США и 163 других стран осознает, что кибербезопасность чрезвычайно важна для выполнения задач и что ключом к успеху деятельности министерства является внимательный и тщательный подбор кадров в сфере кибербезопасности.

Для МО первым принципом является определение главного направления усилий: прием на работу сотрудников, которых в настоящее время министерство формально характеризует как «должности, признанные критически важными для защиты государства, на которых работают сотрудники, которые создают, используют, защищают, охраняют и обеспечивают безопасность киберресурсов МО и США в соответствии со своими должностными обязанностями; они занимаются соответствующей разведывательной деятельностью, готовят будущие операции и демонстрируют силу в киберпространстве и при его помощи».

Это определение еще больше уточняется в Структуре рабочей силы МО в киберсфере (DCWF), которая служит в качестве авторитетного справочного материала для обеспечения всестороннего подхода министерства к управлению профессионалами-кибернетиками из числа военных и гражданских сотрудников, а также нанятых по контракту специалистов. DCWF приносит многостороннюю пользу: она реализует подход, основанный на четком определении должностных обязанностей, применяющийся к идентификации и отчетности по вакансиям при расширенном планировании рабочей силы; она создает единую для всего министерства программу повышения квалификации сотрудников, сосредоточенную на проверке знаний и возможностей кандидатов, на способствовании профессиональному развитию сотрудников и на поддержке продвижения сотрудников по служебной лестнице на основе повышения сложности их должностных обязанностей; она устанавливает основополагающие стандарты для министерства, не основывающиеся на устаревших структурах персонала; и наконец, программа DCWF напрямую поддерживает оперативные нужды и готовность работников, допуская адаптирование и гибкость на уровне их отдельных компонентов.

Для разработки DCWF Министерство обороны использовало Структуру рабочей силы Национальной образовательной инициативы в сфере кибербезопасности (NICE) Национального института стандартов и технологий (NIST), а также Объединенные стандарты обучения и сертификации в сфере киберпространства, изданные Киберкомандованием США. Это позволило министерству навести мост между национальными стандартами и нашими оперативными силами и охватить широкий и разнообразный круг должностных обязанностей – в DCWF содержатся 54 из них – и должностных функций в сфере киберпространства.

Двигаясь дальше, МО признало необходимость в гибкой кадровой системе для гражданских сотрудников-кибернетиков. Действуя в соответствии с документом «Киберстратегия и национальная оборонная стратегия Министерства обороны», выпущенным в 2018 г., и под его влиянием, министерство создало Систему кадров службы за исключением киберспециалистов (CES), призванную решить острые проблемы с принятием на работу, профессиональным ростом и удержанием гражданских сотрудников-кибернетиков в министерстве. CES признает всю сложность нынешнего управления кадрами, предлагая уже готовый профинансированный инструментарий, выходящий за пределы нынешней правительственной практики и системы управления кадрами. Имеются свидетельства того, что те службы, которые перешли на CES, используют эти нововведения с большим успехом в плане заполнения вакансий гражданских специалистов и создания мотивации для профессионалов-компьютерщиков.

Министерство продолжает поддерживать межведомственные инициативы в вопросах рабочей силы в сфере кибербезопасности, активно сотрудничает с NIST и другими федеральными ведомствами, поддерживая NICE, и создает ресурсы, которые используются всеми ведомствами федерального правительства, а также и на общенациональном уровне. Эта работа включает в себя обмен передовым опытом и извлеченными уроками с международными партнерами, стремящимися использовать стандарты NIST при разработке учебных и образовательных программ, часто совместно с Соединенными Штатами. В каждом случае целью является создание разнородной группы, которая бы отвечала за управление, проектирование, защиту, анализ, административную поддержку, деятельность и обслуживание экосистемы правил, механизмов и сетей, от которых зависит наш образ жизни.

Как и в случаях с любыми другими долгосрочными и многоплановыми проблемами, образование и обучение кадров, работающих над этими проблемами, являются ключевым условием их решения – и это особенно верно в отношении проблем в киберпространстве, которое, в конце концов, является сферой, созданной самим человеком. Соединенным Штатам и их союзникам и партнерам требуется дополнительное количество специалистов – как практических работников, так и руководящих сотрудников – которые имеют должное образование и подготовку в сфере кибервозможностей. Например, трудности, вызванные работой из дома из-за нынешней пандемии, еще больше подчеркнули важность прочного механизма обеспечения кибербезопасности, действенных правил «кибергигиены» и широкого распространения базовых знаний об особенностях киберпространства. Чтобы все это начало работать, нам необходимы специалисты-кибернетики в достаточном количестве. Независимо от того, работают ли они в государственном или частном секторе, эти профессионалы находятся на передней линии обороны наших коллективных способностей защищать национальную и экономическую безопасность.

Решая кадровые вопросы в сфере кибербезопасности, необходимо понимать, что не существует какой-то одной проблемы, которая привела к такой ситуации. При наращивании наших трудовых ресурсов в этой сфере мы все сталкиваемся с набором взаимосвязанных моментов, увязывающих воедино среднее и высшее образование, разнородность и инклюзивность, аспекты сертификации и компетентности в кибериндустрии, подбор кадров и их удержание, механизм стажировок и обучения на рабочем месте, национальные правила приема на работу и многое другое. Для того, чтобы переломить нынешние тенденции, необходимы скоординированные усилия как в секторе кибериндустрии, так и в государственном аппарате. С учетом сложности этой проблемы, ее решение зависит от усилий широкого круга заинтересованных сторон.

Таким образом, любая дискуссия на тему наращивания трудовых ресурсов в сфере кибербезопасности представляет собой набор высказанных мнений. Такой обмен мнениями должен проходить как внутри страны, так и с партнерами-единомышленниками в других странах, которые также должны осознавать международную взаимозависимость в киберпространстве и всегда трезво смотреть на существующие и вероятные риски и угрозы. Усилия по улучшению ситуации с трудовыми ресурсами затрагивают ряд технических и производственных областей – от приобретения и модернизации аппаратного обеспечения до необходимых шагов в кадровой политике, таких как обучение, образование, прием на работу и удержание сотрудников – в каждой из которой есть собственные нужды и установившиеся правила. В конечном итоге эти соображения должны занимать приоритетное место в умах руководителей во всем мире, поскольку трудовые ресурсы в сфере кибербезопасности находятся в числе наиболее ценных стратегических активов любой страны. □

**Том Уингфилд –** заместитель помощника министра обороны США. Он оказывает поддержку министру обороны и другим высшим руководителям министерства, формулируя, рекомендуя, интегрируя и реализуя правила и стратегии, направленные на улучшение способности министерства действовать в киберпространстве.

# ДВОЙНОЙ ОБЪЕМ
# ОНЛАЙН

Читайте новые и старые выпуски *per Concordiam*

**https://perconcordiam.com**

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


Еженедельно получайте самые свежие новости о *глобальной безопасности*

transnational
weekly
https://www.marshallcenter.org

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES
DEMOCRATIA PER FIDEM
ET CONCORDIAM

# АКТИВИЗАЦИЯ ЭКОСИСТЕМЫ ТРУДОВЫХ РЕСУРСОВ

## Необходимы партнерство и планирование

**Даниэль Сантос**, менеджер программ, Национальная образовательная инициатива в сфере кибербезопасности, Национальный институт стандартов и технологий при Министерстве торговли США

По мере того, как мир становится более взаимосвязанным при помощи современных технологий, все больше возрастает потребность в трудовых ресурсах, которые бы защищали эти технологии. Однако, исследования показывают, что в сфере кибербезопасности спрос на квалифицированных специалистов превышает предложение. Нехватка работников в сфере кибербезопасности имеет документальное подтверждение. По оценкам доклада «Исследование трудовых ресурсов в сфере кибербезопасности – 2019 г.», необходим глобальный рост числа специалистов в этой сфере в 145%, чтобы удовлетворить нынешний спрос. По данным организации «CyberSeek». org, только в США сегодня остаются незаполненными более 500 тыс. вакансий в сфере кибербезопасности.

Более того, длительный период приема на работу и обучения сотрудников приводит к продолжительным задержкам в функционировании организаций. Как указано в докладе международной профессиональной ассоциации ISACA «Положение дел в сфере кибербезопасности – 2020», почти 30% опрошенных показали, что процесс принятия на работу подходящего сотрудника в сфере кибербезопасности занимает более шести месяцев. Другие 30% опрошенных показали, что заполнение вакансий занимало три месяца. Кроме того, 70% опрошенных считают, что кандидаты в целом недостаточно квалифицированы для занятия этих должностей. Только совместный подход к генерированию высокопрофессиональных трудовых ресурсов в области кибербезопасности поможет в решении этих чрезвычайно важных вопросов.

## Государственно-частное партнерство

Национальная образовательная инициатива в сфере кибербезопасности (NICE) под руководством Национального института стандартов и технологий (NIST) при Министерстве торговли США представляет собой государственно-частное партнерство академических кругов, промышленности и правительственных ведомств. Его задачей является стимулирование и активизация полномасштабного и комплексного образования и экосистемы трудовых ресурсов в сфере кибербезопасности. Именно поэтому NICE с готовностью следует таким идеалам как развитие сотрудничества, совершенствование коммуникаций и обмен ресурсами. NICE функционирует в соответствии со стратегическим планом, разработанным в 2016 г. Принятый в 2014 г. Закон «О совершенствовании сферы кибербезопасности» еще раз подтверждает роль NICE, а параграф IV закона предписывает NIST, как руководящему органу NICE, каждые пять лет разрабатывать и внедрять новые стратегические планы и руководить федеральными программами и мероприятиями с целью поддержки национальной образовательной программы с области кибербезопасности. Закон также обязует NIST «консультируясь с соответствующими федеральными ведомствами, промышленными компаниями, образовательными учреждениями, национальными лабораториями, Программой исследований и разработок в сфере сетевых и информационных технологий и другими организациями, продолжать координировать национальную образовательную программу в сфере кибербезопасности». Далее закон предписывает NIST создавать «поддерживающие официальные образовательные программы в области кибербезопасности на всех образовательных уровнях в целях подготовки и совершенствования профессиональных трудовых ресурсов в сфере кибербезопасности и компьютерной науки для частного сектора и для органов управления на федеральном уровне, на уровне штата, города и племени; и … продвигать инициативы по оценке и прогнозированию будущих нужд работников сферы кибербезопасности в федеральном правительстве и разрабатывать стратегии набора, обучения и удержания персонала».

Стратегический план NICE является результатом сотрудничества и совместного обсуждения всех партнеров NICE в правительстве, академических кругах и в промышленности. В плане отражены видение, миссия, ценности, а также цели и задачи организации. Партнеры NICE будут продолжать работать над эффективными стратегиями реализации, системой показателей и планами, чтобы представить новый пятилетний стратегический план в ноябре 2020 г.

## Видение NICE

Видение NICE заключается в цифровой экономике, приводимой в движение знающим и опытным персоналом в сфере кибербезопасности. Все возрастающая зависимость государственного и частного секторов от жизнестойкого киберпространства для предоставления онлайновых услуг гражданам и потребителям требует комплексных усилий, включающих обеспечение большей степени безопасности данных и компьютерных сетей, чем и должны заняться работники с необходимыми знаниями, навыками и способностями.

## Миссия NICE

Миссия NICE заключается в том, чтобы активизировать и продвигать надежную сеть и экосистему образования, подготовки и развития трудовых ресурсов в сфере кибербезопасности. Хотя аббревиатура NICE подчеркивает компонент образования, подготовка и обучение предоставляют очень важные образовательные возможности, которые реализуются сторонней коммерческой организацией либо самим работодателем. Сертификации, особенно сопровождаемые практическим обучением и оценкой квалификации сотрудника на основе его реально проделанной работы, являются теми показателями, по которым можно проверять знания, навыки и способности персонала. NICE также уделяет большое внимание созданию квалифицированных трудовых ресурсов в сфере кибербезопасности, для чего приоритетом является

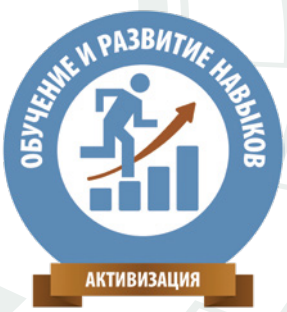
функционирование образовательных учреждений и работодателей в соответствии со Структурой NICE в отношении трудовых ресурсов в сфере кибербезопасности (или Структурой NICE).

## Ценности NICE

Возможно, наиболее важным аспектом разработки стратегического плана был процесс социализации, который привел к образованию общего набора идеалов. *Сотрудничество и коммуникации* находятся в центре усилий NICE по созданию чувства единой общности, которое будет способствовать тому, чтобы все заинтересованные стороны *обменивались ресурсами*. Мы обслуживаем различные сегменты общества и полагаемся на мыслящих руководителей во всех секторах экономики, и поэтому важно, чтобы мы были *моделью инклюзивности* в наших программах и мероприятиях. Мы также хотим быть известными нашей *настойчивой деятельностью* и способностью добиваться результата, и для этого важно, *чтобы мы проверяли гипотезы, искали доказательства и измеряли результаты* нашей работы. Проблемы огромны, нынешнее состояние дел неудовлетворительное, и поэтому мы должны быть готовы *принять перемены* и искать способы *стимулирования инноваций*. Вместе, как единое сообщество, мы добьемся прогресса в ликвидации нехватки квалифицированных специалистов в сфере кибербезопасности, что приведет к повышению уровня экономический и национальной безопасности.

## Цели и задачи NICE

Стратегический план определяет широкий круг целей и задач, которые предполагают определенные шаги и устанавливают приоритеты на следующие несколько лет. Осознавая, что пропасть между постоянно растущим спросом на квалифицированных работников в сфере кибербезопасности и имеющимся предложением становится все шире, первая цель состоит в том, чтобы *ускорить процесс образования и развития навыков* людей. Мы должны сделать так, чтобы и в частном, и в государственном секторах стало понятно, насколько срочно нужно решать проблему нехватки опытных работников в области кибербезопасности. Возможно, реализация именно этой цели и представляет наибольшую проблему, поскольку крайне необходимо найти креативные и эффективные пути увеличения количества нужных специалистов. Эти задачи заставляют нас экспериментировать с новыми подходами, такими как программы стажировок и коллективного обучения, чтобы студенты быстрее переходили из категории учащихся в категорию рабочей силы. Задачи эти также побуждают нас к поиску путей перенаправления вытесненных с рынка работников или работников с неполной занятостью в сторону карьеры в сфере кибербезопасности.



Стратегический план NICE. Цель 1.

Признавая уникальный вклад работников образования, а также различную предыдущую профессиональную подготовку обучающихся, в качестве второй цели мы определили создание общности обучающихся с различной степенью подготовки. Мы стремимся укрепить образовательные и обучающие программы во всей экосистеме, чтобы подчеркнуть важность процесса обучения, оценивать достигнутые результаты и диверсифицировать трудовые ресурсы в сфере кибербезопасности. Вложены значительные инвестиции в образовательные программы, объединение учебных планов, обучение и сертификацию. Тем не менее, мы должны постоянно совершенствовать свою работу с тем, чтобы эти программы приносили ожидаемый результат в плане диверсификации рабочей силы. Центры академического мастерства в сфере кибербезопасности под руководством Агентства национальной безопасности и Министерства внутренней безопасности США и Центры передового технологического образования в сфере кибербезопасности, финансируемые Национальным научным фондом, представляют собой важную основу для дальнейшего развития возможностей и расширения числа участников за счет институтов высшего образования. Хорошо известно, что для того, чтобы поддерживать постоянный приток рабочей силы в сфере кибербезопасности, мы должны знакомить студентов с возможностями трудоустройства еще на ранних стадиях и делать так, чтобы их академическая подготовка в средней школе дала им возможность продолжить образование в институтах и университетах. Среди работников в сфере кибербезопасности недостаточным образом представлены женщины и меньшинства, а также в недостаточной степени используются ветераны отрасли кибербезопасности. Эти тенденции документально подтверждены, и нам необходимо предпринимать конкретные шаги, чтобы их переломить.

Наконец, возможности, предоставленные занятостью в сфере кибербезопасности, дадут сильный толчок экономическому развитию отдельных групп населения, однако работники как государственного, так и частного секторов должны пользоваться какими-то рекомендациями, которые помогут им ориентироваться в постоянно меняющихся карьерных особенностях этой отрасли. И поэтому наша третья цель состоит в том, чтобы *давать рекомендации относительно карьерного роста и планирования трудовых ресурсов*. Профессионалам в области людских ресурсов, менеджерам, отвечающим за набор кадров, и специалистам в сфере кибербезопасности необходима помощь и поддержка в таких вопросах как исследование требований рынка, прием на работу сотрудников, повышение их квалификации и удержание их в штате этих организаций. Компания CyberSeek.org, получающая финансирование от NIST и некоммерческих организаций «CompTIA» и «Burning


Стратегический план NICE. Цель 2.

Glass International Inc.», участвует в выполнении общей задачи по выявлению и анализу источников данных, которые помогают прогнозировать нынешнее и будущее соотношение между спросом и предложением квалифицированной рабочей силы в сфере кибербезопасности. Кроме того, NICE Challenge Project (https://www.nice-challenge.com), разработанный Университетом штата Калифорния в г. Сан-Бернардино, создает набор виртуальных проблемных ситуаций, основываясь на заданиях Структуры NICE. Разработанный Министерством внутренней безопасности США Инструментарий по развитию трудовых ресурсов в сфере кибербезопасности представляет собой пример тех инструментов, которые придут на помощь отделам кадров и менеджерам, отвечающим за набор специалистов.


Стратегический план NICE. Цель 3.

## Совместный подход

Правительственное постановление «Об американской рабочей силе в сфере кибербезопасности», опубликованное 2 мая 2019 г., призывает к налаживанию «консультативного процесса с участием федерального правительства, органов управления на уровне штатов, графств, городов и племен, а также академических кругов, заинтересованных сторон частного сектора и других соответствующих партнеров, в результате которого будет проведена оценка национальных нужд в секторе трудовых ресурсов в сфере кибербезопасности и выработаны рекомендации, а также обеспечена более высокая степень мобильности американских специалистов в сфере кибербезопасности». Имея Рабочую группу NICE, нам не пришлось долго искать существующий механизм для выполнения этого распоряжения.

Созданная в 2015 г. Рабочая группа NICE обеспечивает механизм взаимодействия между представителями частного и государственного секторов с целью выработки концепций и стратегий, а также реализации конкретных мер, которые продвигают образовательные программы в сфере кибербезопасности, и обучение и профессиональное развитие кадров. Рабочей группой руководят три сопредседателя, представляющие, соответственно, академические, промышленные и правительственные круги. Рабочая группа NICE разбита на шесть рабочих подгрупп, работающих с темами и аудиториями, имеющими отношение к таким аспектам как преподавание учащимся предмета кибербезопасности на уровне начальной школы, средней школы и колледжа, организация конкурсов, обучающих программ и механизма сертификации, признаваемого промышленными компаниями, управление трудовыми ресурсами и организация стажировок. Работа каждой из подгрупп, также как и деятельность Рабочей группы в целом, открыта для общественности.

Рабочая группа и ее подгруппы постоянно активно разрабатывают новые проекты и выдают продукты (краткие вводные в проблему на одну страницу, исследовательские доклады, инструментарий, презентации и т.д.), которые являются непосредственным ответом на цели и задачи, определенные стратегическим планом NICE. К рабочей группе часто обращаются за консультациями. Например, поскольку в этом году NICE собирается подготовить обновленный стратегический план, то в каждой подгруппе на совещаниях обсуждаются нужды организации и проводятся «мозговые штурмы» относительно тематики, целей и задач для будущего стратегического плана. Рабочая группа и ее подгруппы были активно задействованы летом 2017 г., когда NICE разрабатывала внутренние процедуры в ответ на правительственное постановление «Об усилении кибербезопасности федеральных сетей и критической инфраструктуры». Это постановление требовало провести оценку «масштабов и достаточности усилий по организации образования и обучения будущих трудовых ресурсов Америки в сфере кибербезопасности, в том числе по разработке учебных планов, относящихся к тематике кибербезопасности, для программ в сфере образования, обучения и стажировки на всех уровнях от начального школьного до университетского» и «предоставить Президенту отчет с выводами и рекомендациями относительно того, как поддерживать рост и самообеспечение национальных трудовых ресурсов в сфере кибербезопасности как в государственном, так и в общественном секторе». В то время результатом консультаций стал «Доклад Президенту о поддержании роста и самообеспечения национальных трудовых ресурсов в сфере кибербезопасности: создание основ для более безопасного будущего Америки» (Доклад о состоянии трудовых ресурсов).

NICE проводит консультации с академическими и промышленными кругами также следующими способами:

- Запрашивает информацию о предлагаемых темах, относящихся к образовательным программам в сфере кибербезопасности и развитию трудовых ресурсов; один из таких запросов был направлен в ответ на Правительственное постановление №13800, требовавшее «информации о масштабах и достаточности усилий по организации образования и обучения национальных трудовых ресурсов в сфере кибербезопасности и рекомендаций относительно того, как поддерживать рост и самообеспечение национальных трудовых ресурсов в сфере кибербезопасности как в государственном, так и в общественном секторах».

- На рассмотрение общественности постоянно предоставляются черновые версии публикаций NICE, в том числе и «Специальная публикация NICE 800-181», которая определила Структуру NICE в отношении трудовых ресурсов в сфере кибербезопасности.
- Сотрудничество с Консультационным советом NIST по вопросам информационной безопасности и конфиденциальности информации, созданным в соответствии с Законом о федеральном консультативном комитете (FACA) для предоставления NIST консультативных услуг в вопросах информационной безопасности и конфиденциальности.
- Мнения Консультативного совета по политике трудовых ресурсов США, еще одной группы в составе FACA, которая предоставляет консультации и рекомендации межведомственному совету, возглавляемому Министерством торговли США в соответствии с Правительственным распоряжением «О создании президентского национального совета, защищающего интересы американских рабочих».
- Другие общественные форумы или консультативные советы, созданные для помощи другим правительственным министерствам и ведомствам.
- Участие в мероприятиях, финансируемых грантами NIST, таких как ежегодная Конференция и выставочная экспозиция NICE, Конференция NICE по образованию по предмету кибербезопасности в средних школах и симпозиумах Центра академического мастерства в сфере кибербезопасности, проводимых ежегодно сразу после проведения конференций и выставочных экспозиций NICE.
- Приглашения в качестве выступающих или гостей на встречи, проводимые академическими или промышленными кругами, или мероприятия, на которых сотрудники NICE имеют возможность услышать и узнать о назревающих вопросах, появляющихся возможностях и новых программах в организациях как государственного, так и частного сектора.

Представители общественности приглашаются принять участие в функционировании Рабочей группы NICE, присутствуя на конференциях или других мероприятиях, спонсируемых NICE, в том числе на встречах, где обсуждаются вопросы образования и рабочей силы, имеющие отношение к сфере кибербезопасности.

NICE также сотрудничает и с правительственными организациями. Межведомственный координационный совет NICE собирает своих партнеров из федеральных правительственных ведомств для консультаций, обмена мнениями и координации политических инициатив и стратегических направлений, относящихся к программам образования, обучения и развития рабочей силы, связанных с кибербезопасностью. На регулярно проводимых встречах этой группы Отдел текущих программ NICE делится с партнерами из федеральных ведомств последними новостями, а также узнает о том, как работа этих ведомств поддерживает усилия NICE. Эта группа также определяет и обсуждает вопросы проводимой политики и стратегических направлений в работе NICE.

## Единый стержень

Структура NICE в отношении трудовых ресурсов в сфере кибербезопасности была сформирована таким образом, чтобы создать единый язык для категоризации и описания деятельности в сфере кибербезопасности и предложить инструменты для определения стартовых возможностей и профессиональных недостатков персонала, а также для обеспечения постоянного притока квалифицированных работников в области кибербезопасности. Первая версия Структуры NICE была опубликована в 2012 г. и превратилась в своего рода национальный стандарт для работодателей, практических работников и работников образования, обучающих инструкторов и слушателей в общественных, частных и академических кругах. В других странах этот документ также используется в качестве справочного материала. По мере того, как все больше организаций приводят свои усилия в области развития трудовых ресурсов к единой классификации, результатом станут более стандартизированные трудовые ресурсы в сфере кибербезопасности, которые смогут более эффективно защищать наши компьютерные сети и системы.

Последняя версия Структуры NICE была опубликована в августе 2017 г. как «Специальная публикация NICE №800-181». Эта версия расширила первоначальный лексикон документа и включает более точную


Источник: Отдел реализаии программ NICE

классификацию категорий направлений работы в сфере кибербезопасности, области специализации, а теперь еще и роли, которые они выполняют. «Специальная публикация NICE №800-181» также стала первой версией, в которую включены детали по таким категориям работ как «Сбор и использование данных» и «Анализ данных» с описанием необходимых знаний, навыков, способностей и выполняемых задач. В предыдущих версиях информация по этим категориям была убрана, поскольку была чрезвычайно специализирована и чувствительна. Последняя версия предлагает более детальную информацию об особенностях этой работы и дает возможность работникам образования и инструкторам готовить работников именно в этих областях.

Структура NICE будет и дальше меняться в соответствии с нуждами тех групп потребителей, которых она обслуживает. NICE стремится динамично поддерживать актуальность, применимость и полезность этого документа, в то же время совершенствуя его соответствие существующим стандартам, рекомендациям и другим структурам. Сохранение актуальности Структуры NICE чрезвычайно необходимо для подготовки нашей национальной рабочей силы к работе в области кибербезопасности, которая становится все более сложной. Именно поэтому мы начали цикл регулярных обновлений и в ноябре 2019 г. объявили о планах опубликовать пересмотренную версию «Специальной публикации NICE №800-181». Перед опубликованием мы представили общественности черновой вариант документа с просьбой направить свои комментарии.

Обновления Структуры NICE будут происходить при сотрудничестве с частным сектором и другими правительственными ведомствами в духе транспарентности, открытости и партнерства.

Изменения в Структуре NICE будут основываться на комментариях тех субъектов, которые используют этот документ и применяют его на практике. Те, кто занимается планированием трудовых ресурсов, а также работники образования, инструкторы, работодатели и обучаемые работники могут высказать пожелания включить в Структуру NICE новые компоненты или информационные материалы. Когда мы активно привлекаем представителей частного и государственного секторов к выработке стандартов, таких как Структура NICE, мы полагаемся на экспертов со всей страны – и со всего мира – и используем их для повышения качества, актуальности и вероятного применения нашего конечного продукта. О необходимости отдельных улучшений мы узнаем из отзывов тех, кто нас консультировал, реализовывал или применял Структуру NICE или участвовал в составлении этого документа. Примерами таких улучшений могут быть проведение аудитов персонала, описание должностных обязанностей, четкое определение ожидаемого конечного результата обучения, проверка знаний, навыков и способностей, а также создание путей карьерного продвижения для тех, кто проходит обучение или ищет работу.

## Вместе мы сильнее

В сентябре 2016 г. Отдел текущих программ NICE выделил финансирование организации под названием «Региональный альянс и многостороннее партнерство во имя стимулирования развития образования и трудовых ресурсов в сфере кибербезопасности» (RAMPS) для пяти пилотных программ. Эти программы нацелены на то, чтобы свести вместе работодателей, испытывающих нехватку специалистов в сфере кибербезопасности, с работниками образования с тем, чтобы сформировать профессиональные кадры, отвечающие нуждам промышленности отдельных городов и целых регионов. Одно из требований программы заключалось в том, чтобы каждый участник мог подтвердить наличие партнера среди местных работодателей и как минимум в одном из следующих учебных заведений: средняя школа, местный отдел образования или высшее учебное заведение (колледж, институт или университет).

Посредством разработанной системы показателей создание программ RAMPS продемонстрировало, что региональные альянсы и партнерства могут положительно влиять на увеличение трудовых ресурсов в сфере кибербезопасности. Все большее количество студентов решает прослушать соответствующие курсы, все большее число работников понимают возможности сделать карьеру в этой области и все большее количество людей хотят пройти интернатуру по этой специальности. Это свидетельствует о том, что создание партнерских отношений может существенно изменить экосистему трудовых ресурсов в сфере кибербезопасности. Как сказала Хелен Келлер: «В одиночку мы можем сделать так мало, но вместе мы способны сделать так много».

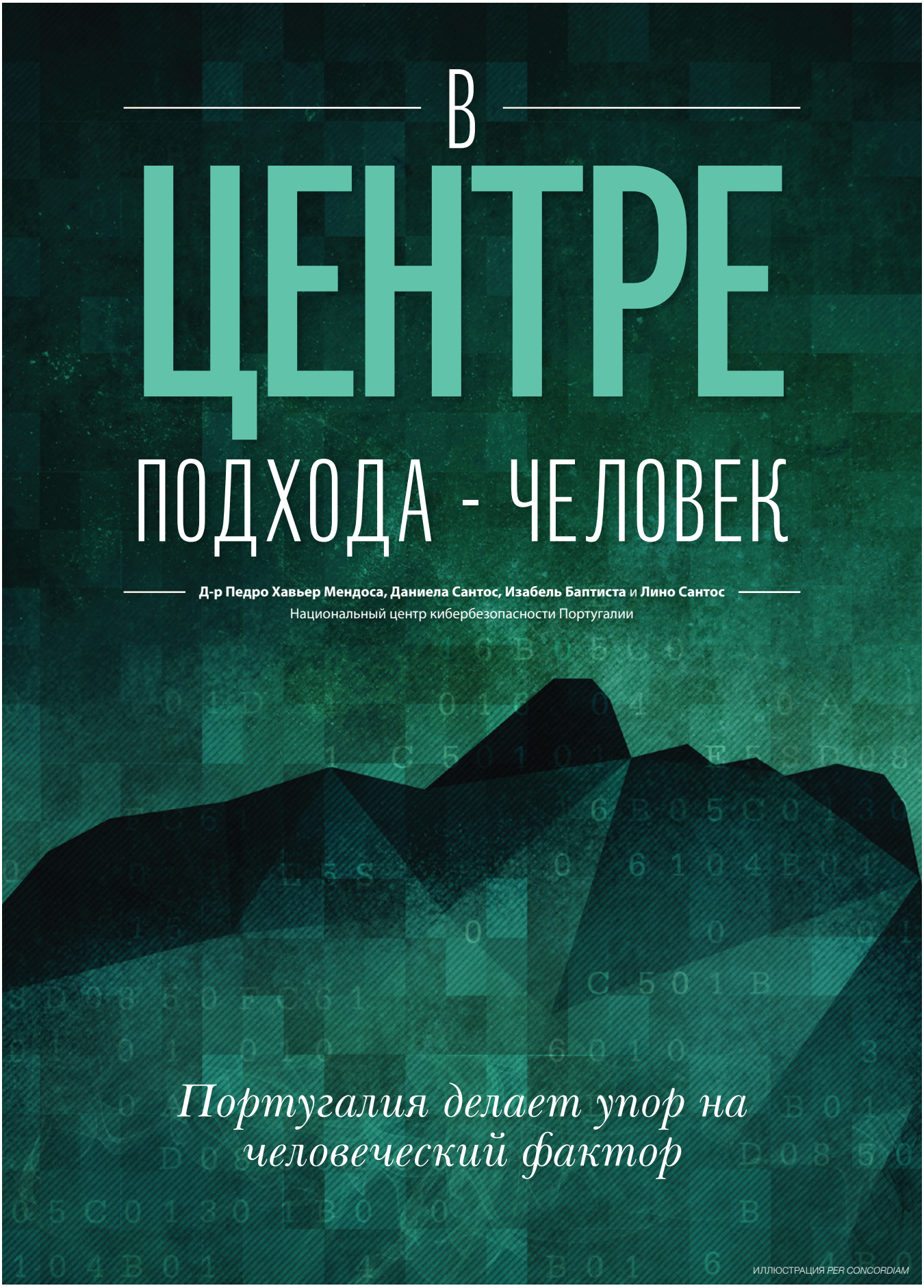
## Дополнительные публикации

Нижеперечисленные документы ни в коем случае не являются исчерпывающим списком публикаций. Тем не менее, они дают более детальный контекст для тех программ, подходов и материалов, которые описаны в этой статье.

- NICE Cybersecurity Workforce Framework (https://nist.gov/nice/framework)
- A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce (https://doi.org/10.6028/NIST.IR.8287)
- Report on the International Workshop on Cybersecurity Education and Workforce Development Capacity Building (https://www.nist.gov/document/nice-international-workshop-report-2019)
- NICE Strategic Plan (https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan)
- Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/report) □

# В ЦЕНТРЕ ПОДХОДА - ЧЕЛОВЕК

**Д-р Педро Хавьер Мендоса, Даниела Сантос, Изабель Баптиста** и **Лино Сантос**
Национальный центр кибербезопасности Португалии



*Португалия делает упор на человеческий фактор*

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

Термин «кибербезопасность» представляется несколько расплывчатым. В докладе Агентства кибербезопасности Европейского союза (ENISA) «Различия и совпадения в определении кибербезопасности в процессе стандартизации» говорится, что различные международные институты стандартов используют разные значения этого термина. Они разнятся от «конфиденциальность, целостность и доступность информации» в киберпространстве (Международная организация по стандартизации – ИСО) и «набор инструментов, правил, концепций и гарантий безопасности, рекомендаций, подходов к управлению рисками, мероприятий, программ обучения, передового опыта, мер страхования и технологий, которые могут использоваться для защиты киберсреды, а также активов организации и пользователя» (Международный союз электросвязи – МСЭ) до «способность защищать или оборонять использование киберпространства от кибератак» (американский Национальный институт стандартов и технологий – NIST). Эти различные точки зрения особое значение придают защите информации и сетей, причем некоторые из них ограничиваются только угрозами, исходящими из интернета (NIST), в то время как другие охватывают и все возможные виды угроз (МСЭ).

Мы признаем эти различные определения, но при этом считаем, что кибербезопасность выходит далеко за пределы информационной безопасности. Такие события, как скандал с фирмой «Cambridge Analytica», показывают, что кибербезопасность должна учитывать слабые стороны общественного устройства, вызванные изменениями в том, как люди общаются между собой, потребляют информацию и действуют. Поэтому важно и дальше совершенствовать нынешние определения этого термина, например, данное МСЭ, и сделать именно человека центральным элементом кибербезопасности. Информация и сети, которые мы стремимся защитить, принадлежат людям и являются творением человеческой воли и деятельности. И когда мы поставим в центр нашего подхода именно человека, то важность развития трудовых ресурсов существенно возрастает. Человеческий элемент не должен быть второстепенным или равнозначным другим аспектам кибербезопасности; наоборот, он должен быть центральным компонентом, вокруг которого должны объединиться все остальные. Этот подход не следует интерпретировать таким образом, что он принижает значение технических аспектов, защиты информации или архитектуры компьютерных систем. Он просто подразумевает, что все эти элементы должны рассматриваться с точки зрения человеческого фактора. Например, информационная система может иметь современную защиту от вирусов, но в то же время ее архитектура все же может нести угрозу ключевым ценностям организации или общества.

Подход к кибербезопасности, в центре которого находится человеческий фактор, также подразумевает преодоление подхода, в центре которого находится национальная безопасность, и при котором кибербезопасность рассматриваются с точки зрения национальной территории и ее жизненно важных услуг. Такому пониманию свойственно реалистичное толкование безопасности, указывающее на угрозы, представляющие объективную опасность для национального суверенитета. Человекоцентричный подход основывается на индивидуумах и их сетях общения, представляя собой концепцию кибербезопасности, основывающуюся на человеческом факторе и теории космополитизма. В отличие от доводов реалистов, этот подход признает конструктивистский характер безопасности в качестве сферы, определенной выражением воли социальных субъектов в процессе секьюритизации, выбирающей и включающей различные области в зависимости от предполагаемой ситуации – тезис, соответствующий трансверсальной и многосторонней природе кибербезопасности. Таким образом, аспект развития трудовых ресурсов в организации кибербезопасности должен занять центральное место, поскольку он признает важность человеческого фактора, учитывает необходимость совершенствования навыков для эффективной защиты людей и призывает к выработке стратегий, направленных на распространение кибербезопасности путем идентификации поведения в качестве вектора, являющегося основным «связным» с другими векторами.

## СТРАТЕГИЯ ПОРТУГАЛИИ

В Португалии прилагаются большие усилия для выработки общественной политики в сфере кибербезопасности. В этом процессе центральную роль играет принятая в 2019 г. Национальная стратегия Португалии в сфере безопасности киберпространства, являющаяся второй по счету стратегией в этой области в Португалии. Первая стратегия была принята в 2015 г. Стратегия 2019 г. совершенно четко признает важность развития трудовых ресурсов. В этой стратегии заложено несколько осей воздействия. В числе наиболее важных и, конечно же, имеющих больше всего направлений действий, находится ось, относящаяся к «предотвращению, обучению и информированности». Развитие трудовых ресурсов включено в три сферы воздействия: обучение и переквалификация специалистов, обучение и информированность руководителей и повышение уровня информированности общественности. Признавая трансверсальный характер цифровой трансформации и, соответственно, ее человекоцентричную нагрузку, эта стратегия способствует внедрению образовательных и обучающих программ, дающих работникам первоначальную квалификацию или обеспечивающих их переквалификацию как в организациях, занимающихся вопросами кибербезопасности, так и в масштабах широкой общественности, частного сектора и общественного управления, включая поставщиков жизненно важных услуг. С ее помощью также можно выделить одаренных работников в ходе соревнований с заданием «захвати

флаг», а также в ходе компьютерных учений на национальном уровне и на уровне отдельных организаций.

Для того, чтобы определить, реализовать и оценить стратегию, мы должны установить точку отсчета, реально отображающую нынешнюю ситуацию, отслеживать действия по выбранным направлениям и смотреть, выполняются ли поставленные задачи. Исходя из этих соображений, португальский Национальный центр кибербезопасности (CNCS) создал Наблюдательный центр по кибербезопасности, задача которого заключается в том, чтобы удовлетворять эти потребности, а также накапливать знания о состоянии кибербезопасности в стране, используя междисциплинарный метод, охватывающий различные области, в которых человек выступает в качестве ключевого элемента кибербезопасности.

Развитие трудовых ресурсов является центральным аспектом. Наблюдательный центр разрабатывает и собирает показатели количества проведенных в Португалии курсов по вопросам кибербезопасности, количества человек, прослушавших эти курсы, процента женщин, прошедших обучение, уровня занятости в каждой области с учетом спроса и предложения, количества записавшихся на неформальные обучающие курсы и других аспектов, дающих информацию о развитии трудовых ресурсов. Эти знания являются частью того, что можно назвать «триангуляцией», включающей в себя исследования и развитие, знания и становление трудовых ресурсов. Центр способствует проведению исследований и развитию, распространяя знания, которые могут быть использованы для достижения реальных и полезных для общества результатов, например, для разработки программ развития рабочей силы.

## УЧЕНИЯ И ПРОГРАММА ОБУЧЕНИЯ И ПОВЫШЕНИЯ ИНФОРМИРОВАННОСТИ

Одними из ключевых аспектов стратегии CNCS по развитию трудовых ресурсов являются киберучения и Программа обучения и повышения информированности, в которых участвуют все заинтересованные стороны. Учения проводятся ежегодно, и на каждом из них ставится цель обучить отобранных сотрудников из критически важных организаций моделям поведения в конкретных ситуациях. Например, в 2019 г. в стране прошли три различных выборных кампании, которые и стали темой киберучений, на которых отрабатывалось реагирование на гипотетические кампании дезинформации. С этой целью к учениям привлекли несколько организаций, в том числе Национальную избирательную комиссию и Регулирующее агентство для СМИ Португалии. Обмен совместно полученным опытом на этом уровне способствовал улучшению подготовки профессионалов к реагированию на киберинциденты в ходе выборов и передаче информации этим организациям.

Программа обучения и повышения информированности предоставляет работникам и менеджерам уникальную возможность для повышения своей квалификации. Планируется проводить усовершенствование квалификации специалистов, однако пока что эта сфера деятельности в основном реализуется при помощи структур и инструментов под эгидой CNCS. Первоначальный проект Программы обучения и повышения информированности был представлен на рассмотрение работникам образования, исследователям и бизнес-институтам. Окончательный проект включал в себя сделанные предложения, которые относились к трем основным направлениям: масштабные открытые курсы в режиме онлайн (MOOC) по вопросам кибербезопасности для всех работников, но также и для отдельных институтов; курсы обучения инструкторов, на которых будут обучаться и затем оцениваться сотрудники различных организаций, которые затем сами будут обучать других сотрудников, таким образом расширяя круг кадров, прошедших обучение; и очные обучающие сессии для работников общего профиля и руководителей старшего звена.

В 2019 г. в рамках направления MOOC был разработан курс «Гражданин в кибербезопасности». Это бесплатный простой курс с рекомендациями относительно практических шагов в сфере «кибергигиены», и его слушателями являются простые граждане из состава рабочей силы различных пересекающихся секторов экономики. В первый год в нем приняли участие более 30 тыс. граждан, и примерно 20 тыс. из них успешно прослушали весь курс. Основываясь на их отзывах, содержащих замечания и пожелания, была определена тематика следующих курсов MOOC: дезинформация, покупки в режиме онлайн и безопасное использование социальных сетей.

Модель «Обучение инструкторов» требует сотрудничества со стороны работников – в основном, из учреждений общественного управления и крупных компаний – которые становятся частью большой группы инструкторов, использующих материалы CNCS для проведения обучающих занятий по кибербезопасности у себя в организациях. Эта модель была представлена всем заинтересованным сторонам как общественный долг без каких-либо затрат. Являясь поставщиком жизненно важных услуг и объектом многих кибернападений, сектор здравоохранения стал одним из первых и наиболее заинтересованных участников этой программы обучения. По тем же причинам Налоговая служба также стала важным партнером. Большую важность представляют университеты, поскольку они хорошо осознают необходимость в повышении информированности и обучении персонала учебного заведения и местных жителей, в среде которых они функционируют. Чем дальше вглубь страны, тем большую роль играют эти институты в экономическом и социальном развитии, а также в развитии трудовых ресурсов.

Если говорить о формальном образовании, CNCS оказал помощь в разработке профессионального курса совместно с несколькими заинтересованными сторонами, названного «Технический сотрудник сферы

кибербезопасности». Основываясь на списке слабых мест, обнаруженных в сфере компьютерной безопасности группой реагирования «Национальная сеть» в ходе своей деятельности, CNCS также подготавливает аспирантские и специализированные курсы (очные и в режиме онлайн) с наиболее обновленным содержанием, как того требует процесс развития рабочей силы в этой сфере знаний.

## СТРУКТУРЫ И ИНСТРУМЕНТЫ

Еще одним важным компонентом стратегии CNCS по развитию трудовых ресурсов является четкое понимание того, что автономные и независимые организации должны предпринимать шаги для достижения максимально высокого уровня зрелости своей кибербезопасности. Для этой цели CNCS создал структуры и инструменты, ориентирующие все организации на обеспечение полного соответствия требованиям – от первых шагов до самого высокого уровня. Национальный справочник по вопросам кибербезопасности является одним из таких документов и, возможно, наиболее важным. Основываясь на международных стандартах, таких как ISO 27001 и NISTSP-800-53, он дает четкие указания относительно того, что организация должна делать, чтобы обнаруживать инциденты, защищаться от них, реагировать на них и восстанавливаться с учетом национальных реалий и возможных дополнительных сведений о других международных стандартах. Одна из поставленных целей – развитие трудовых ресурсов со ссылками на Программу обучения и повышение информированности и дополнительные потребности в обучении, определяемые рынком. В качестве первого шага в развитии трудовых ресурсов CNCS предоставляет документ «Дорожная карта к минимальным возможностям в кибербезопасности», который позволяет субъектам с начальным этапом развития структур в этой сфере достичь минимально необходимого уровня кибербезопасности. Этот документ особенно важен для организаций малого и среднего размера с ограниченными ресурсами в сфере кибербезопасности.

## ПРОБЛЕМЫ И РЕКОМЕНДАЦИИ

Подход CNCS начинается с концептуального уровня, затем переходит на стратегический и завершается операционализацией по двум направлениям: обучение и структуры для автономных действий. Эти два направления пересекаются в том смысле, что обучение должно отражать структуры, а последние должны включать в себя обучение как часть процесса обеспечения соответствия стандартам.

На сегодняшний день наибольшего успеха удалось добиться в аспекте распространения знаний благодаря Программе обучения и повышения информированности, продемонстрировавшей, что гражданское общество с готовностью приняло этот вид деятельности. Кроме того, успеха удалось добиться в динамике создания структур, в котором участвовали отдельные заинтересованные стороны, и в ходе которого происходил очень интересный процесс адаптации международных стандартов к контексту Португалии. Это сплотило все заинтересованные стороны, что, в свою очередь, укрепило всю систему в целом.

Одна из основных проблем развития трудовых ресурсов состоит в необходимости расширении возможностей подготовки технического персонала в ответ на требования, порождаемые современными технологиями, а также в насущной потребности переквалификации профессионалов в сфере информационных технологий (ИТ) в специалистов в области кибербезопасности. Еще одна серьезная задача состоит в том, чтобы настойчиво доказывать центрам профессиональной подготовки, средним школам и университетам важность разработки большего количества курсов и введения их в учебные программы по ИТ предметам, относящихся к кибербезопасности. В центрах профессиональной подготовки и в средних школах также важно вводить предметы, относящиеся к кибербезопасности, с целью повышения информированности и пробуждения интереса молодых людей к этой сфере, в которой они смогут выбрать свою будущую специальность. Значительную трудность представляет также переход от разработки структур к практической деятельности. Учитывая ограниченность имеющихся ресурсов, здесь потребуются крупные вложения со стороны частного бизнеса и гражданского общества.

Для того, чтобы применять передовой опыт в сфере развития трудовых ресурсов, национальные ведомства, отвечающие за кибербезопасность, должны максимально вовлекать в решение этой задачи все заинтересованные стороны. На то есть две причины: во-первых, заинтересованные стороны лучше других в состоянии определить свои нужды и потребности и во-вторых, их участие вызывает у них мотивацию и порождает чувство ответственности, что повышает качество результатов их работы. В числе заинтересованных сторон должны находиться известные представители академических кругов, квалифицированные специалисты в сфере кибербезопасности и промышленные ассоциации. Кроме того, при создании структур необходимо ставить развитие трудовых ресурсов на одно из первых мест, а также задействовать школы и обучающие организации для обеспечения распространения специализированного обучения и переквалификации.

Развитие кадров в сфере кибербезопасности, как потребность, в которой пересекаются много аспектов, должно реализовываться по восходящему принципу с использованием всех субъектов, которые могут получить от этого пользу. С этой точки зрения, в этом процессе необходимо поставить во главу угла именно человеческий фактор, определив аспекты безопасности, включая кибербезопасность, на то место, которое они заслуживают – внесение вклада в обеспечение более безопасной и процветающей жизни всех людей на земле. □

СТИМУЛИРУЯ

# ЧАСТНЫЙ СЕКТОР

## КАК ПРАВИТЕЛЬСТВЕННЫЕ ЗАКАЗЫ МОГУТ УКРЕПИТЬ КИБЕРБЕЗОПАСНОСТЬ

**Ацуко Секигучи**, заместитель советника, Международная стратегическая группа, Национальный центр обеспечения готовности к инцидентам и стратегии кибербезопасности (NICS) и секретариат кабинета министров Японии

**Подготовка трудовых ресурсов в сфере кибербезопасности является насущным вопросом как в Японии, так и во всем мире. В соответствии с данными доклада «Исследование трудовых ресурсов в сфере кибербезопасности – 2019 г.», опубликованного Международным консорциумом сертификации безопасности информационных систем, в мире сейчас имеется более 4 млн. свободных вакансий по этой специальности. В азиатско-тихоокеанском регионе нехватка составляет 64% от необходимого количества работников. В Японии, по данным Организации азиатско-океанской компьютерной индустрии за 2018 г., в 2016 г. нехватка квалифицированных специалистов составляла 132 тыс. человек, и предполагалось, что к 2020 г. эта цифра возрастет до 193 тыс.**

**Уважая независимость субъектов частного сектора, Япония политику развития трудовых ресурсов реализует через добровольные инициативы. Например, наращивание трудовых ресурсов в сфере кибернетики в соответствии с принятой в 2018 г. Стратегией кибербезопасности осуществляется путем повышения уровня информированности населения, расширения образовательных возможностей, повышения квалификации на протяжении всей профессиональной карьеры и совершенствования системы сертификации.**

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

И все же, широко признается нехватка квалифицированных работников, что показывает ограниченность возможностей добровольных инициатив. Одним из вариантов повышения эффективности реализации принятой политики может быть введение обязательных мер по примеру Соединенных Штатов, где введен в действие Президентский указ «О трудовых ресурсах Америки в сфере кибербезопасности», изданный в 2019 г. Этот указ требует, чтобы все компании, получающие государственные заказы, внедрили структуру, разработанную Национальной образовательной инициативой в сфере кибербезопасности (NICE) и предусматривающую распределение ответственности в сфере укрепления кибербезопасности и карьерный рост специалистов в этой области.

Первая часть этой статьи разъясняет суть нынешней политики Японии по расширению трудовых ресурсов для частного сектора и приводит последние данные относительно кадров в сфере кибербезопасности. Во второй части рассматривается американский вариант введения обязательных мер по наращиванию трудовых ресурсов. В заключительной части рассматривается возможность использования американского сценария в Японии и предлагается вариант, подходящий для реалий Японии.

## СИТУАЦИЯ В ЯПОНИИ

В качестве исторической основы политики кибербезопасности в Японии служил «Основной закон о создании общества развитых информационных и телекоммуникационных сетей», принятый в 2000 г., статья 22 которого содержит общие положения об обязанности правительства принимать меры по обеспечению безопасности телекоммуникационных сетей. Это означает, что в этом законодательном акте, направленном на ускорение развития и внедрения цифровых технологий, об информационной безопасности почти ничего не сказано и не содержится упоминание о сторонах, заинтересованных в этом процессе. Нынешняя политика Японии в сфере кибербезопасности отражена в «Основном законе о кибербезопасности», принятом в 2014 г. Статья 4 этого закона предписывает правительству разработать политику в области кибербезопасности и внедрить ее на территории всей страны. Статьи 6, 7 и 8 обязывают операторов объектов критически важной инфраструктуры, частные компании и частные организации, работающие в компьютерной сфере, сотрудничать с правительством в достижении цели национальной политики в сфере кибербезопасности. Статья 22 прямо требует от государства принятия конкретных шагов по развитию трудовых ресурсов в области кибербезопасности путем введения соответствующих поощрений квалифицированных специалистов, использования систем сертификации и обучения молодежи при сотрудничестве учебных заведений и частных предприятий. Это означает, что закон распределяет обязанности между всеми заинтересованными сторонами, участвующими в

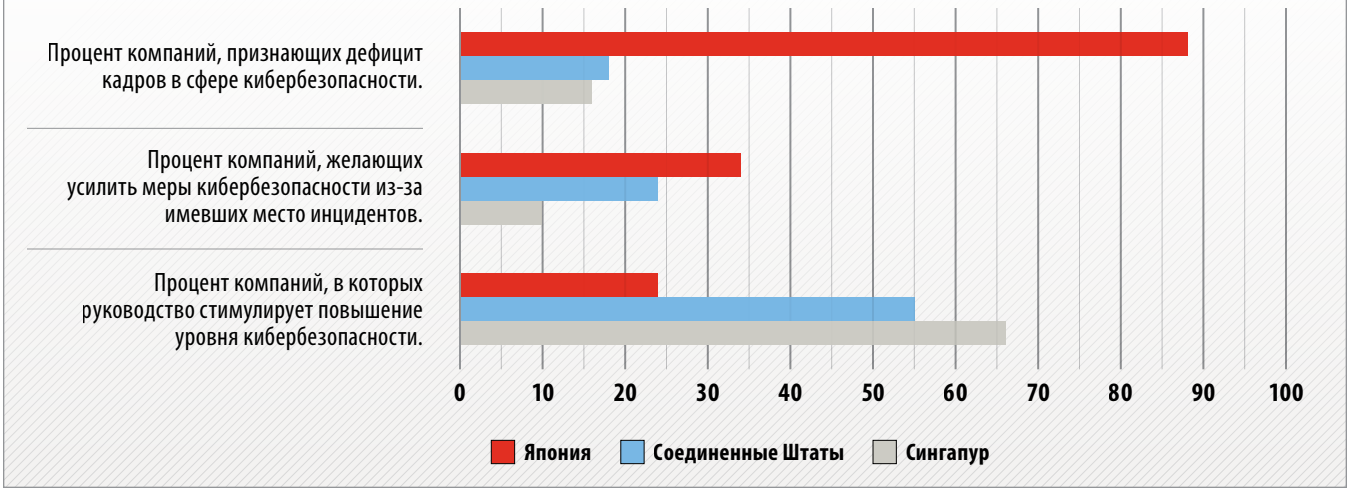
**Дефицит рабочей силы в сфере кибербезопасности по регионам**


Источник: доклад «Исследование трудовых ресурсов в сфере кибербезопасности – 2019 г.», опубликованный Международным консорциумом по сертификации безопасности информационных систем

развитии трудовых ресурсов, но при этом, уважая независимость необщественных организаций, для частного сектора эти обязанности не делаются обязательными.

Обязанности правительства юридически закреплены, но при этом конкретные меры, которые оно будет предпринимать, в законодательстве не отражены. Таким образом, Стратегия кибербезопасности и сопутствующие документы определяют основные положения политики в области кибербезопасности. Законодательство требует, чтобы в качестве наивысшего органа принятия решений в отношении политики кибербезопасности был создан Стратегический штаб кибербезопасности. Он должен состоять из соответствующих политических деятелей, представителей академических кругов и профессионалов из частного сектора и отвечать за выработку стратегии кибербезопасности. Самая последняя стратегия кибербезопасности, принятая в 2018 г., имеет три основных составляющих: экономическая жизнеспособность, общественная безопасность и международная стабильность. Один из разделов документа посвящен наращиванию трудовых ресурсов как фактору, проходящему красной нитью через все три составляющие. В этом разделе указывается на необходимость реализации политики на всех уровнях – в частном секторе, учебных заведениях и в правительственных кругах. В отношении стратегии, в 2018 г. Стратегический штаб кибербезопасности предложил ввести Инициативу развития трудовых ресурсов в сфере кибербезопасности. В этой инициативе указаны конкретные меры в отношении частных организаций: повысить информированность руководителей путем распространения рекомендаций относительно политики кибербезопасности; создать работникам возможности переквалифицироваться и подняться по карьерной лестнице до руководящих должностей; и создать соответствующие технические

Сравнительный анализ признания проблем в сфере кибербезопасности – Япония, США и Сингапур




Источник: «NRI Secure Insight 2019»

возможности посредством введения системы сертификации. Таким образом, в политике развития трудовых ресурсов в отношении частных компаний выработан подход, основанный на создании в них благоприятных условий для повышения уровня информированности и профессионализма.

Помимо того, что, согласно статистическим данным, дефицит рабочей силы в Японии растет, исследование «NRI Secure Insight 2019» показало, что 87,8% компаний в Японии признают факт нехватки кадров в сфере кибербезопасности, в то время как этот показатель в США составляет 18,1%, а в Сингапуре 16,3%. Правительство Японии принимает меры по развитию трудовых ресурсов путем расширения возможностей и образовательных перспектив, но при этом в стране все равно широко признается дефицит кадров по этой специальности.

Хотя японское правительство реализует политику по повышению информированности в частном секторе, данные NRI свидетельствуют о том, что реальным стимулом к повышению уровня кибербезопасности является понесенный в результате инцидентов ущерб, а не действия руководства компаний. В этой связи возникают вопросы относительно нынешних добровольных инициатив и относительно того, являются ли они достаточными для того, чтобы справиться с недостатком людских киберресурсов в частном секторе.

## ПРИМЕР СОЕДИНЕННЫХ ШТАТОВ

В США в отношении наращивания трудовых ресурсов в сфере кибербезопасности действуют обязательные правила. В частном секторе есть много проектов, направленных на достижение трех целей, определенных Стратегическим планом NICE, принятым в 2012 г.: ускорение процесса обучения и приобретения профессиональных навыков; стремление к разнообразию в среде обучаемых; и предоставление направляющих рекомендаций относительно карьерного развития и планирования в кадровой сфере. За этим документом последовал Президентский указ 2017 г. «Об усилении кибербезопасности федеральных сетей и критической инфраструктуры», который предписывает министру торговли и министру внутренней безопасности докладывать о ситуации с развитием трудовых ресурсов. Одно из направлений деятельности – внедрение Структуры NICE в отношении трудовых ресурсов в сфере кибербезопасности («Специальная публикация 800-181»), принятой Национальным институтом стандартов и технологий, входящим в Министерство торговли США. Этот документ принят с целью четкого распределения должностных обязанностей трудовых ресурсов в сфере кибербезопасности и разбивает виды работ на семь категорий: обеспечение безопасности, эксплуатация и обслуживание, осуществление мониторинга и управления, охрана и защита, проведение анализа, сбор и обработка данных и проведение расследований. В пределах этих категорий обозначены 33 специализации и 52 функциональные обязанности. Кроме того, Президентский указ «О трудовых ресурсах Америки в сфере кибербезопасности», вступивший в силу в 2019 г., в законодательном порядке требует от частных компаний, получающих государственные заказы, применять у себя эту структуру с целью ее максимально широкого продвижения.

## ЯПОНИЯ И ВВЕДЕНИЕ ОБЯЗАТЕЛЬНОГО ПРИНЯТИЯ МЕР

Подойдет ли для Японии американская схема законодательного принуждения частных компаний к принятию определенных мер? В том, что касается аспекта определения возможностей в сфере кибербезопасности, Форум обнаружения киберрисков в ключевых секторах совместно с американской инициативой NICE разработал Справочник терминов в сфере трудовых ресурсов. Этот Форум состоит из нескольких десятков национальных компаний и отделений зарубежных компаний из секторов химической промышленности, финансовых институтов, промышленного производства, средств массовой

информации и транспортных услуг. Справочник определяет задачи, которые необходимо решить для обеспечения кибербезопасности, ответственных за решение каждой задачи, а также необходимый уровень знаний. Процесс подготовки этого справочника позволил прийти к единому пониманию кибербезопасности между специалистами из разных секторов экономики с разными бизнес-культурами и разными взглядами на проблему развития трудовых ресурсов. Таким образом, японская структура развития рабочей силы в сфере кибербезопасности была разработана не правительством, а организацией, поддерживаемой частным капиталом, что демонстрирует уважение к независимости частного сектора.

Национальным центром обеспечения готовности к инцидентам и стратегии кибербезопасности (NISC) на основании статьи 25 в качестве мандата от Стратегического штаба безопасности на создание стандартов оценки мер, принимаемых правительственными ведомствами, были приняты «Единые стандарты мер в сфере информационной безопасности для правительственных ведомств и связанных с ними учреждений» (Единые стандарты). На основе этих документов ведомства установили свои собственные стандарты кибербезопасности, а NISC проверяет их с целью убедиться, что Единые стандарты неукоснительно соблюдаются и обеспечивают установленный уровень безопасности правительственных ведомств. В разделе 4 содержатся условия, которые должны быть включены в процесс размещения государственных заказов. Хотя в Единых стандартах содержатся технические условия, позволяющие избежать слабых мест в контактах между правительственными ведомствами и частными компаниями, в число критериев не входит условие развития кадров в частных компаниях.

Короче говоря, между США и Японией существуют различия. В США эта структура встроена в процесс размещения правительственных заказов с целью принудить частные компании принять ее в своих организациях. А в Японии требование реализации частными компаниями политики развития трудовых ресурсов не входит в число условий размещения госзаказов. Кроме того, хотя и был проведен анализ ситуации с трудовыми ресурсами с учетом культурных особенностей Японии, по-прежнему сохраняется зависимость реального использования результатов этого анализа от инициатив частных организаций. Таким образом, из-за существования многочисленных различий, введение американской практики в Японии затруднено и нецелесообразно.

Кроме того, внедрение требования к частным компаниям относительно развития трудовых ресурсов как условия размещения государственных заказов может привести к дискуссиям о том, допускается ли это дополнительное условие положениями Всемирной торговой организации о второстепенных условиях. Эти положения ограничивают введение условий участия на основе «юридических и финансовых способностей и коммерческих и технических возможностей выполнить соответствующий госзаказ». Неясно, будет ли требование развивать трудовые ресурсы входить в число таких условий, но этот вопрос выходит за рамки данной статьи.

Хотя введение в Японии Справочника терминов в сфере трудовых ресурсов в качестве правомочного требования и не проходило гладко, при распределении госзаказов правительство в состоянии проводить сравнительный анализ заявок от частных компаний с целью убедиться в необходимом качестве предоставляемых услуг. При этом используется несколько оценочных критериев, такие как предложенная цена, качество предложения и соответствующий опыт компании, с тем, чтобы, соблюдая общественные интересы, отдать заказ достойному претенденту. Если принятие мер по развитию трудовых ресурсов, например, внедрение структуры людских ресурсов, станет одним из критериев оценки при распределении госзаказов и найдет отражение в Единых стандартах, то это подтолкнет частные компании к тому, чтобы сделать этот аспект приоритетным. Это также не оставит никаких сомнений в соответствии международному торговому режиму, поскольку предприятия будут подталкиваться к принятию таких мер, но ни одному предприятию не будет отказано в возможности подать заявку на госзаказ. Кроме того, этот шаг действительно приведет к ускорению развития трудовых ресурсов в частных кампаниях помимо добровольных инициатив, но все же будет уважать независимость частного сектора, что является принципиальным для политики кибербезопасности в Японии. Некоторые могут критически отнестись к этой идее, поскольку компании, работающие над госзаказами, составляют относительно небольшой процент от общего числа частных компаний. Тем не менее, было бы вполне реалистично для правительства в качестве первого стимулирующего шага сделать принятие мер по развитию трудовых ресурсов одним из оценочных критериев при рассмотрении заявок на госзаказы, а соответствующее условие закрепить в Единых стандартах. Более того, это предложение можно было бы расширить и на другие компании, связанные с компанией, подающей заявку на госзаказ.

## ЗАКЛЮЧЕНИЕ

Одной из возможных мер, стимулирующей частные предприятия в Японии внедрить у себя планы развития рабочей силы, могло бы стать, помимо добровольных инициатив, введение соответствующего условия в процесс подачи заявок на госзаказы. Возможно, предложенные меры не приведут к немедленному изменению политики всех частных компаний. И все же это предложение вызовет дополнительные дискуссии, причем не только в Японии, но и в других странах, относительно того, как государство может перестать полагаться исключительно на добровольные инициативы и начать улучшать ситуацию с развитием трудовых ресурсов в сфере кибербезопасности на благо будущих поколений. □

Данная статья отражает исключительно мнение автора и не представляет официальную позицию NISC или правительства Японии.

# *В состоянии* ГОТОВНОСТИ

## СОВЕРШЕНСТВУЯ НЕМЕЦКИЙ КИБЕРРЕЗЕРВ

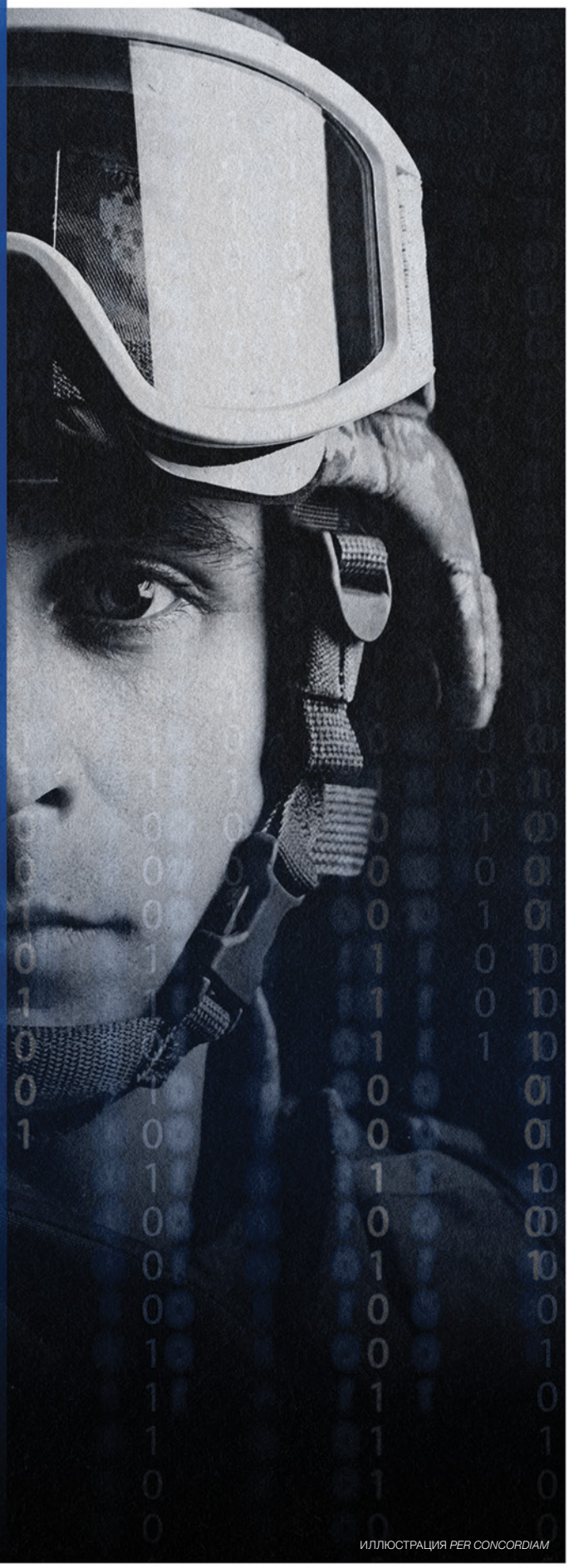


ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

**Руперт Брандмайер, Йорн-Александр Хей, д-р Флориан Рупп** и **Клеменс Войвод** –
офицеры запаса, германская Служба кибернетики и информатики

После распада Советского Союза в 1991 г. напряженность между восточным и западным политическими блоками быстро и существенно снизилась. Вследствие этого политики в объединенной Германии все чаще стали подвергать сомнению необходимость обязательной военной службы, и в 2011 г. она была сначала приостановлена, а затем и почти вовсе отменена. После этого Бундесвер превратился в армию на добровольной основе, постоянно сталкивающуюся с растущей проблемой набора в свои ряды необходимого количества подходящих для службы новобранцев. В связи с этим в последние годы возросло значение сил резерва и стала популярной идея передачи части ответственных задач от военнослужащих действительной службы резервистам. Краеугольным камнем соответствующего генерального плана Министерства обороны (МО) является призыв на службу квалифицированных резервистов-кибернетиков.

Военная служба информатики и кибернетики (MCS) занимается организацией всех аспектов службы резервистов по специальности «кибернетика». MCS является самым молодым подразделением федеральных сил обороны Германии, которые также включают в себя Сухопутные силы, ВМФ, ВВС, Объединенные силы обеспечения и Объединенную медицинскую службу. В ведении MCS находятся подразделения, отвечающие за компьютерные и информационные технологии (ИТ), военную разведку, геоинформацию и оперативные коммуникации. В отличие от традиционных видов войск, MCS в основном работает в автономном режиме.

Доклад «Состояние дел в сфере кибернетики и информатики», подготовленный Министерством обороны в 2016 г., определил основы формирования и функционирования военного резерва специалистов-компьютерщиков, сформулировав три главные цели:

1. Создание дополнительных сил, способных оказать поддержку MCS в случае крупномасштабной кибератаки.
2. Создание квалифицированных киберподразделений, состоящих из экспертов в области ИТ, путем проведения совместных учений отдельными группами.
3. Укрепление сотрудничества и диалога между экспертами ИТ в частном, общественном и военном секторах.

Министерство обороны понимает, насколько важны квалифицированные кадры в деле укрепления кибербезопасности. Для того, чтобы сделать для соответствующих критериям призывников службу в действующих подразделениях или в резерве привлекательной, Бундесвер предлагает три пути, в основе каждого из которых лежит компонент образования: принять новую программу кибербезопасности, предлагаемую Университетом Бундесвера; ввести особую модель призыва для специалистов-компьютерщиков, которые не хотят проходить военную службу в традиционном ее понимании; и увеличить набор резервистов, особенно экспертов ИТ. Последние два пути представляют определенную проблему из-за неоднородной структуры распределения «ноу-хау» информационных технологий как в обществе в целом, так и среди резервистов. Более того, кадры MCS и опытные специалисты-резервисты могут установить связь с общественностью путем проведения бесед, групповых дискуссий и других мероприятий с целью вызвать интерес либо к действительной службе в подразделениях MCS, либо к поступлению в резерв в качестве специалиста по кибертехнологиям.

## СТРУКТУРА КИБЕРОБОРОНЫ

В анализе, проведенном Центром исследований проблем безопасности при Университете Цюриха в апреле 2020 г., сравнивались силы киберрезерва Эстонии, Финляндии, Франции, Израиля, Швейцарии и США. Исследование пришло к выводу, что организационные формы киберрезерва в этих странах существенно различаются из-за культурных особенностей бюрократического аппарата и вооруженных сил. Хотя во Франции,

США и Нидерландах армии создаются на добровольной основе (как и в Германии), исходные условия для создания киберрезерва довольно сильно разнятся из-за особенностей систем образования, военных структур и состояния рынка рабочей силы.

В Германии создание нового киберрезерва привязано к образованию региональных отделений MCS. Помимо штаб-квартиры резерва MCS созданы еще четыре региональных центра резервистов с целью улучшения связи с резервистами-компьютерщиками, живущими в этих регионах. Эти центры, расположенные в районах, где проживают специалисты по ИТ, должны принимать на работу опытных резервистов, которые будут проходить службу на ротационной основе. Такой подход дает необходимые знания и опыт на региональном и местном уровнях, которых в противном случае в распоряжении вооруженных сил не было бы.

В нынешней ситуации пандемии COVID-19 становится очевидной еще одна выгода от децентрализации резерва MCS – геостратегический фактор. Подразделения регулярных войск и резервистов в отдельных регионах страны могут быть не в состоянии выполнять свои обязанности на необходимом уровне эффективности, хотя это может и не отразиться на других частях страны. Задачи могут быть переданы полностью боеготовному региональному центру MCS, который сможет быть доукомплектован дополнительными сотрудниками, что позволит устранить любые недостатки в работе.

Принимая во внимание основные цели Министерства обороны страны, задачи центра резерва MCS начинаются с создания привлекательных для резервистов возможностей обучения одновременно с организацией, проведением и последующим анализом киберучений, в которых будут присутствовать как аспект учебных программ (такие как контент), так и аспект логистики. Сюда входит организация конкурсов по тематике кибербезопасности как на объекте, так и в онлайновом режиме, с тем, чтобы привлечь внимание одаренных специалистов в области компьютерных технологий и стимулировать их интерес к военной карьере. Для поддержки соответствующих учебных курсов и учений потребуется специальное программное и аппаратное обеспечение (своего рода «киберполигон»). Для начала MCS предлагает, чтобы каждый резервист-компьютерщик, в зависимости от опыта в ИТ, подходил для работы в одной из следующих пяти основных областей:

- **«Красная команда»:** имитация хакерской атаки с целью проверки жизнестойкости компьютерной инфраструктуры.
- **Киберразведка:** сбор информации об угрозах для того, чтобы снизить риски кибернападения.
- **Мониторинг:** отслеживание сетей, пользователей и вебсайтов с целью определить слабые места и угрозы.
- **Разведданные в открытых источниках (OSINT):** просмотр общедоступных интернет-источников в поисках информации.
- **Киберпреступления и ответные действия в случае инцидентов (DFIR):** анализ цифровых компонентов с целью обнаружения противозаконной деятельности и принятия надлежащих ответных мер в случае доказанного киберпреступления.

Другие области, как, например, те, которые связаны с задачами MCS в сфере геоинформации, могут быть определены на более позднем этапе. Каждый региональный центр должен будет определить, какими именно навыками должен обладать потенциальный резервист для того, чтобы соответствовать нуждам конкретной зоны ответственности, а затем будет обобщать данные по квалификации каждого резервиста. Совместно с штаб-квартирой MCS региональные центры создадут наборы общих и индивидуальных квалификационных требований к служащим резерва. Когда резервиста отберут для обучения в одной из пяти областей, MCS составит под него индивидуальную программу обучения, которая подготовит из резервиста эксперта в этой области.

В случае киберинцидента эксперты в каждой из пяти областей должны будут объединить свои взаимодополняющие опыт и знания. Такая возможность снизить киберриски и способность к сотрудничеству могут быть проверены в конкурсах специалистов в сфере кибербезопасности. Кроме того, резервисты должны будут оказывать поддержку в таких областях как системное администрирование, оценка надежности и жизнестойкости аппаратного обеспечения и программных продуктов, установка безопасных сетей и защита существующей инфраструктуры ИТ. Резервисты должны быть знакомы с организационными и коммуникационными аспектами (связь с общественностью), быть способными распознать «фейковые новости» и поддерживать на должном уровне свою осведомленность в вопросах информационной безопасности. И наконец, по всем вопросам, касающимся образования резервистов в сфере кибернетики, региональные центры резервистов сотрудничают с соответствующими организациями, такими как Командно-штабное училище Бундесвера (Führungsakademie), Университет Бундесвера, полицейские академии, а также с гражданскими учреждениями. В частности, региональные центры организуют публичные мероприятия, такие как беседы, пропагандирующие возможности, раскрывающиеся перед перспективными кандидатами, если они присоединятся к MCS или киберподразделениям резерва.

Функциональные возможности системы резерва MCS могут проверяться в ходе конкурсов специалистов в сфере кибербезопасности, проводимых на национальном или международном уровне с задействованием участников из частного, общественного и военного секторов. Конкурсы могут включать ситуацию «захвата флага», задания по выявлению угроз, стресс-тесты по обнаружению слабых мест, позволяющие проникнуть в систему, а также имитацию нападения и защитных мер. Некоторые сценарии для таких конкурсов будут разрабатываться

**Рисунок 1:** Важные сферы обучения резервистов-кибернетиков


Резервисты-кибернетики пройдут обучение в таких областях как кибератаки, шпионаж и похищение информации, превентивная защита от угроз, социальная инженерия, манипуляции с аппаратным обеспечением и хакерская деятельность.

таким образом, чтобы правильное решение нашел один участник, а другие будут предполагать работу команды экспертов в различных областях, каждый из которых будет отвечать за свой участок.

## КОНЦЕПЦИЯ ОБУЧЕНИЯ РЕЗЕРВИСТОВ

Ключевая роль резервных военных киберподразделений состоит в том, чтобы во время кризисной военной ситуации (включая кибернападения) в оперативном порядке предоставить специалистов, которые бы компенсировали нехватку экспертов на действительной службе в Бундесвере. Одна из причин сложностей с набором на действительную службу достаточного количества специалистов-кибернетиков состоит в том, что примерно 30 других федеральных и региональных учреждений, занимающихся вопросами кибербезопасности – такие как федеральное Управление безопасности информационных технологий и отделы кибербезопасности в региональных и федеральных управлениях криминальных расследований – полагаются в работе на тех же самых экспертов.

Источником дополнительных трудностей является частный сектор. На рисунке 1 дается сравнение ключевых возможностей специалистов, работающих над компьютерными проблемами в промышленном и военном секторах. «Отчет АНБ», опубликованный в 2017 г. «Corporate Trust GmbH» – немецкой компанией, занимающейся управлением рисками – содержит детальное описание этих возможностей. Мониторинг, как одна из основных областей, имеет прямое отношение как к промышленному, так и к военному сектору. Это означает, что MCS будет пытаться мотивировать промышленных экспертов в этой области перейти на службу в группу мониторинга военного подразделения резерва. В случае приема на службу экспертов в области мониторинга не будет необходимости в масштабном обучении этих новых специалистов, поскольку требования в этой сфере в промышленном и в военном секторах схожи.

Кроме того, значительную часть «требуемого военного «ноу-хау» в сфере кибернетики» невозможно получить из частного сектора по той простой причине, что его там нет. Например, в промышленном секторе трудно найти экспертов, которые бы вошли в «Красную команду» (команду хакеров). Совершенно очевидна необходимость соответствующего повышения квалификации и подготовки резервистов-кибернетиков. В частности, подготовка специалистов для «Красной команды» будет представлять существенную трудность, поскольку хакерская деятельность не может официально входить в список служебных обязанностей и не существует формальных путей получения образования по этому предмету.

Основываясь на анализе желаемых возможностей и имеющихся в наличии ресурсов, могут быть разработаны узкоспециализированные курсы и определены конкретные знания и навыки, которые требуются той или иной команде специалистов. В контексте пяти групп экспертов, из которых будут сформированы команды специалистов, следует отметить, что для членов каждой группы достаточно получить чисто теоретические знания в некоторых из 15 областей кибернетики, определенных на рисунке 1, в то время как в отдельных критически

важных областях помимо прочной теоретической основы требуется и практический опыт компьютерных операций.

В таблице 1 для пяти групп экспертов в качестве примеров даны задания на теоретическую и практическую компетентность в шести выбранных областях кибернетики. Важно, чтобы для оценки имеющихся возможностей применялись объективные, поддающиеся контролю критерии. С этой целью каждый резервист-кибернетик, до того, как начать программу обучения, должен будет пройти тест на профессиональное соответствие. Анализ расхождения между необходимыми и имеющимися навыками работников позволяет определить количество участников индивидуальных курсов, учебные программы, а также место и время их проведения.

Как уже отмечалось, подготовка членов «Красной команды» будет особенно необходима, поскольку для подразделений киберрезерва будет трудно найти кандидатов с опытом хакерских атак на достаточно высоком уровне.

На рисунке 2 в качестве примера показана программа, на основе которой MCS может составить график обучения будущих членов «Красной команды».

В этом примере после завершения программы обучения резервист станет экспертом в трех наиболее востребованных отраслях «хакерской науки»: использование Интернета, реверсивное проектирование программного обеспечения и использование системы двоичных кодов. В соответствии с примером, приведенным на рисунке 2, этот конкретный работник должен будет повысить уровень подготовки в сферах использования Интернета и реверсивного проектирования программного обеспечения, в то время как в сфере использования системы двоичных кодов никакое обучение в ближайшее время требоваться не будет.

Для кандидатов в «Красную команду», желающих стать специалистами во всех трех областях, создаются особые модели обучения. В специальности по использованию Интернета обучающиеся должны достичь уровня эксперта в области проверки возможности проникновения в систему, т.е. в ходе смоделированного кибернападения определить уязвимые места компьютерной системы. В вводных теоретических курсах неопытного слушателя ознакомят с платформой KALI Linux и более чем с 600 инструментами кибернападения, которые она предлагает. В качестве следующего шага учащиеся примут участие в занятиях, на которых будет продемонстрировано, как инструменты KALI Linux могут применяться для решения задач, поставляемых сервером «Взломай коробку». Для того, чтобы перейти на следующий уровень, будут проводиться семинары, включающие лекционный компонент и практические упражнения, на которых будут показываться решения задач типа «захвати флаг» при поддержке инструментария Juice Shop – открытого проекта по безопасности веб-приложений.

Ключом к реверсивному проектированию программного обеспечения является анализ программ с целью выделить из них дизайн и имплементирующую информацию. Для того, чтобы стать кандидатом на обучение в этой области, работник в качестве предварительного условия должен быть знаком с языками программирования Java

**Таблица 1**

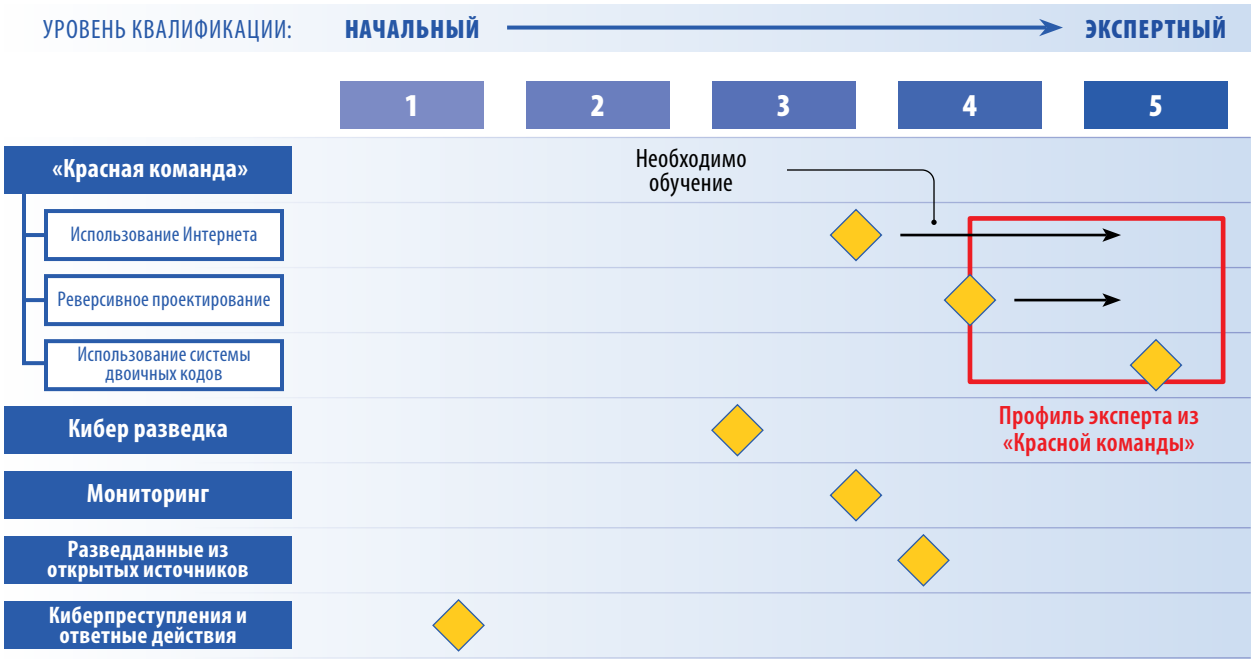
| | Хакерство | Кибер пропаганда | Мониторинг | Активная оборона | Манипуляции с аппаратным обеспечением | Шпионаж/ похищение информации |
|---|---|---|---|---|---|---|
| **«Красная команда»** | П | Т | Т | Т | Т | Т |
| **Киберразведка** | Т | П | Т | Т | Т | П |
| **Мониторинг** | Т | Т | П | Т | Т | Т |
| **Поиск разведданных в открытых источниках** | Т | П | Т | Т | Т | Т |
| **Реагирование на криминальную деятельность в цифровом пространстве** | Т | Т | Т | Т | П | П |

Источник: авторы статьи

**Т** = теоретическая компетентность **П** = практическая компетентность

В этой обзорной статье проводится различие между группами резервистов с практической (П) и теоретической (Т) компетентностью в шести из 15 областей кибернетики, показанных на рисунке 1. Теоретическая компетентность в определенной сфере может быть достигнута путем посещения соответствующих лекций. Практическая компетентность в конкретной сфере требует как теоретической подготовки, так и реального практического опыта компьютерных операций.

**Рисунок 2:** Определение индивидуального графика обучения




Источник: авторы статьи

В данной версии программы для определения учебного расписания резервиста готовят к тому, чтобы он стал членом «Красной команды» или экспертом-хакером. Как показано, компетентность в хакерской деятельности можно подразделить на три области. Первоначальный уровень квалификации резервиста, обозначенный желтыми ромбами, определяется тестом на компьютерные знания до того, как будет выработана индивидуальная программа обучения.

и Assembler. В вводных курсах будут сочетаться лекции на тему реверсивного проектирования и исправления машинного кода и байт-кодов Java и практические занятия. Последующие семинары продемонстрируют, как в теории, так и на практике, как навыки в реверсивном проектировании могут быть использованы для снижения рисков, связанных с вирусами.

Наконец, в использовании системы двоичных кодов манипулирование с двоичными кодами преследует цель получить доступ к защищенной информации. Обычно это уже более сложный предмет изучения и относится к языку программирования среднего уровня, такому, как язык C, и знание низкоуровневого языка Assembler является обязательным для этого курса подготовки. Здесь на лекциях сначала расскажут об уязвимых функциях языка C, использовании простых брешей, структуре Global Offset Table, введенных в системы смягчающих элементах и о важности возвратно-ориентированного программирования с целью избежать использования смягчающих элементов. Затем у слушателей будет возможность применить эти методы к бинарным кодам. В дальнейшем занятия будут сосредоточены на повреждении компьютерной памяти, начиная с объяснений того, как использовать переполнение Windows, и с последующим переходом к инструкциям по использованию Интернет-браузеров. В процессе обучения будут сочетаться лекции и практические занятия.

## ЗАКЛЮЧЕНИЕ

Министерство обороны Германии в 2016 г. признало, что с основными вызовами обществу и вооруженным силам в сфере безопасности могут справиться военные резервисты-кибернетики. Более того, считается, что эти резервисты играют очень важную роль в повышении информированности общества в вопросах кибербезопасности. Министерство обороны признает, что создание резервных подразделений, специализирующихся на кибербезопасности и способных оказать эффективную поддержку MCS, потребует значительных усилий по набору достаточного количества соответствующих требованиям резервистов и организации их дальнейшего обучения. В ответ на эти потребности создается новая организационная структура кибероборонs с целью укомплектовать MCS резервистами-компьютерщиками. Региональные центры резерва MCS будут распределены по всей стране с тем, чтобы усовершенствовать механизм набора резервистов и обеспечить постоянное повышение их квалификации. В этой статье мы изложили план подбора «идеальной группы» киберэкспертов с различными специализациями. Из этого пула резервистов MCS будет создавать команды, соответствующие требованиям MCS по повышению безопасности ИТ и противодействию различным киберугрозам. □

# ПОТРЕБНОСТЬ В «СУПЕРГЕРОЯХ» АНАЛИТИКИ

## Обращаясь к нетехническим аспектам киберугроз

**Ондрей Ройчик**
руководитель отдела стратегической информации и анализа, Национальное управление кибернетики и информационной безопасности Чехии

Мы склонны рассматривать кибербезопасность как чисто технический вопрос. В последние годы десятки докладов указывают на нехватку экспертов в области кибербезопасности, что объясняется в целом недостаточным количеством специалистов с образованием в сфере информационных технологий. Упор на относительную нехватку технических экспертов, однако, представляется довольно узким подходом, который не принимает в расчет потребность в специалистах других категорий, у которых опыт и образование не являются чисто техническими. Например, на рынке труда востребованы менеджеры в сфере кибербезопасности, аудиторы, юристы, эксперты в области внутренней и международной безопасности, специалисты по региональным проблемам, работники образования и аналитики. Нетехнические аналитики занимаются контекстуализацией инцидентов в сфере кибербезопасности и текущими тенденциями, и именно эту функцию в течение последних четырех лет неоднократно выполняло Национальное управление кибернетики и информационной безопасности Чехии (NÚKIB). Какими же профессиональными навыками должен обладать сотрудник, чтобы стать нетехническим аналитиком в сфере кибербезопасности?

### Контекстуализация

В декабре 2018 г. NÚKIB выпустило предупреждение относительно использования технологий китайских телекоммуникационных компаний «Хуавей» и «ZTE». В предостережении говорилось, что использование продуктов этих компаний представляет угрозу безопасности, поскольку китайское законодательство требует от китайских граждан и компаний сотрудничества с государственными органами, включая разведывательные службы. После получения такого предупреждения системные администраторы критически важных объектов в Чешской Республике по закону обязаны признать наличие такой угрозы и принять соответствующие меры.

NÚKIB также является активным сторонником Пражских инициатив – схемы кибербезопасности, появившейся в результате конференции по вопросам безопасности технологий 5G, проведенной в Праге в 2019 г. Основная идея Пражских инициатив заключается в том, что помимо технической природы киберугроз при оценке безопасности информационных технологий необходимо принимать во внимание особые политические, экономические и иные действия злоумышленников. У кибербезопасности есть политические аспекты. В Чехии опыт анализирования нетехнических/контекстуальных сторон кибербезопасности привел к появлению многочисленных сторонников такого инклюзивного подхода к кибербезопасности.

Ситуация с технологиями «Хуавей» и «ZTE» и Пражские инициативы были не первыми случаями, когда NÚKIB видело необходимость в развитии нетехнических аналитических возможностей при решении вопросов, относящихся к кибербезопасности. С 2015 г. агентство проводит детальные тренинги для руководящих работников, в основном из государственных учреждений. Один из важных выводов, полученных в ходе этих тренингов, состоит в том, что изучение одних только технических деталей инцидентов без анализа более широкого контекста делает почти невозможным для ответственных руководителей определение и принятие соответствующих ответных мер и выбор оптимального направления действий.

### Внутренние аналитические возможности

Для предоставления контекстуальной информации и анализа всех обстоятельств относительно конкретной кибератаки и юридического, политического и экономического окружения отдельных субъектов необходимо собрать все соответствующие данные и иметь сложные аналитические процедуры и навыки. Будет крайне непрактичным полагаться на внешних партнеров, таких как разведслужбы или частные компании. У разведслужб отсутствует гибкость в двух аспектах: во-первых, у них редко есть именно та информация, которая в данный момент необходима, и во-вторых, большинство информации засекречено, что создает трудности в ее немедленном получении и использовании. Что касается частных компаний, то государственной организации


Источник: автор статьи

сложно доверять субъекту из частного сектора и в своих действиях полагаться исключительно на информацию, полученную от него. Тем не менее, информация, предоставленная частной компанией, может внести определенный вклад в общую копилку данных на более поздней стадии аналитического процесса.

Вот уже более четырех лет NÚKIB создает собственные нетехнические аналитические возможности в сфере кибербезопасности. Их основная задача в том, чтобы поддерживать установленный рабочий цикл и предоставлять аналитические материалы по вопросам кибербезопасности ключевым руководящим работникам в правительстве и других стратегически важных учреждениях. На самом деле NÚKIB является национальным агентством в области кибербезопасности в Чехии. Помимо других сфер деятельности, агентство отвечает за выработку политики и правил, относящихся к кибербезопасности. Для того, чтобы принятые правила и процедуры отражали текущую ситуацию, ежедневно должен проходить процесс обновления информации и «сканирования горизонта». Любое государственное учреждение с общенациональными полномочиями в сфере кибербезопасности получит пользу от обладания такими возможностями.

NÚKIB извлекает выгоды из того, что персонал, отвечающий за технические аспекты, и специалисты в области политики и существующих правил работают под одной крышей. Это эффективно работающая схема, однако в силу организационных или исторических причин она может оказаться неподходящей для многих стран. Во многих национальных экосистемах кибербезопасности эти две составные части кибербезопасности разделены, если они вообще существуют. Может существовать на национальном уровне независимая компьютерная группа реагирования на чрезвычайные ситуации (CERT) в то время как политическими аспектами кибербезопасности занимаются в министерстве внутренних дел, в министерстве промышленности или ином ведомстве. Если специалисты по политическим вопросам создают подразделение по кибербезопасности в одном из этих министерств, то это подразделение будет анализировать только стратегические тенденции. Если такое подразделение создано в составе технической службы – CERT – то естественным стремлением будет обращать основное внимание только на контекстуализацию конкретных технических инцидентов.

При любой схеме аналитический отдел должен быть составной частью организации. Аналитический аспект работы должен пронизывать всю организацию и охватывать инфраструктуру полностью – базы данных, аналитическое программное обеспечение и сотрудников. Специальные отделы, генерирующие соответствующие данные, должны обмениваться этими данными с аналитиками, которые потом смогут их связать с данными, полученными из других частей организации и с более широким контекстом внешних тенденций. Такой обмен данными между различными частями организации чрезвычайно важен. Если данные не объединяются в единый пул, то тогда знания становятся изолированными в стенах разных отделов организации, что в результате приводит к снижению ценности данных и неудовлетворительному качеству аналитики.

## Считайте это отдельным проектом

Любая организация, заинтересованная в создании специализированного аналитического подразделения для оценки нетехнических аспектов киберугроз, должна принимать во внимание множество факторов. В их числе – высокоспецифичные профессиональные навыки аналитиков. Однако, все эти ключевые условия должны быть соблюдены еще до того, как начнут подбираться сотрудники.

Отнеситесь к созданию нетехнического аналитического подразделения как к отдельному проекту. Для успешного выполнения этого проекта крайне важно определить цели, которых вы хотите достичь, например, какой вид услуг будет предоставляться и кому. Ключевой аспект такого проекта заключается в том, чтобы найти целеустремленного спонсора, известного на жаргоне руководителей проектов как «спонсор». Внутри

организации этот убежденный сторонник проекта является его разработчиком, ожидает от него существенной пользы и стремится к его полной реализации. Роль спонсора не сводится к просто официальному представительству. Эффективное спонсорство возможно лишь тогда, когда спонсор лично убежден в ценности проекта и стремится продвигать его и поддерживать участвующих в нем сотрудников всеми официальными и неофициальными способами на всех стадиях реализации проекта.

Необходимо иметь абсолютно четкое представление о процессе создания аналитического подразделения, чтобы доказать вышестоящему руководству организации необходимость выделения ресурсов. Высококачественные аналитические подразделения стоят недешево, необходимы большие затраты на аналитическое программное обеспечение, возможности сбора и хранения данных, получение данных, а также на текущее обслуживание и другие периодически необходимые процедуры. И конечно же, штат сотрудников нового подразделения. Помимо зарплат, будут затраты на их постоянное обучение и образование. Любому проекту необходим менеджер, отвечающий за координацию, но еще больше нужны сотрудники, которые осознают свою миссию и не только поддерживают ее, но и постоянно совершенствуют внутренние процедуры и аналитическое мастерство подразделения.

## Необходимая компетентность

Для эффективного функционирования аналитической единицы необходима слаженная работа двух групп сотрудников – аналитиков и команды, отвечающей за сбор данных и поддержание аналитического программного обеспечения. Для каждой из этих двух групп требуется специфический набор навыков и знаний. У аналитиков должны быть глубокие знания в вопросах национальной и международной безопасности. В отдельных случаях необходимо, чтобы их знание проблем региона подкреплялись владением несколькими иностранными языками. Они должны иметь базовые знания в технических аспектах кибербезопасности, а также знать основные правила и процедуры, относящиеся к информационной безопасности. Еще одним необходимым элементом этой работы является искусство анализа разведданных, инструменты и приемы анализа разведданных из открытых источников (OSINT), а также знание аналитического программного обеспечения, поддерживаемого группой сбора данных. В свою очередь, в группе сбора данный должны быть специалисты двух категорий – разработчики данных с опытом управления крупными инфраструктурами данных и ученые с глубокими знаниями в таких областях как интегрирование данных, информатика и инструменты визуализации данных.

Что касается должностей аналитиков, то нынешний рынок труда вряд ли сможет предоставить кандидатов с полным набором необходимых знаний и навыков, и поэтому будет необходимо идти на компромисс и

**НАЧАЛЬНИК АНАЛИТИЧЕСКОГО ОТДЕЛА**

| Аналитическое подразделение | Подразделение сбора данных |
|---|---|
| • Эксперты по региональной безопасности<br>• Эксперты по вопросам международной безопасности | • Разработчики данных<br>• Ученые, специализирующиеся на обработке данных |

определять ключевые профессиональные качества, к которым потом будут прибавляться новые. Для дальнейшего профессионального развития необходимы следующие ключевые условия: безграничная пытливость и энтузиазм в отношении предмета своей деятельности; желание постоянно учиться чему-то новому; способность постигать сложные и эволюционирующие концепции; способность понять взаимосвязь между киберпространством и физическим миром; профессиональные навыки письменных и устных презентаций на родном языке; хорошее знание английского языка, а если речь идет об исследовании конкретного региона, то и приличное знание языка, доминирующего в этом регионе. Имея эту основу, уже можно будет добавлять другие навыки и знания.

Будучи относительно небольшой организацией, NÚKIB активно использует обучение сотрудников на рабочем месте, а также внешние тренинговые программы, предоставляемые Школой НАТО в г. Обераммергау, натовским Центром мастерства в области совместной кибероборонь, а также частными компаниями. В течение примерно трех лет сотрудники проходят обучение по таким аспектам как OSINT, аналитические навыки, разведдеятельность и киберугрозы, специализированное программное обеспечение и иностранные языки. В этот период у всех аналитиков есть достаточно возможностей принять участие в десятках аналитических проектов и в расследовании серьезных инцидентов и реагировании на них, а также создать собственную сеть коллег для межведомственного сотрудничества. После достаточного периода такого повышения квалификации может рассматриваться вопрос о переводе сотрудника на должность старшего аналитика.

Профессиональное совершенствование в сфере кибербезопасности представляет собой нескончаемый процесс, поскольку все приобретенные сегодня знания в вопросах OSINT, разведки и киберугроз, аналитического программного обеспечения и т.д. через два или три года рискуют стать устаревшими. Для того, чтобы идти в ногу с развитием кибербезопасности, мировой политики и некоторых других ключевых сфер, помянутых выше, нужно быть поистине супергероем аналитической работы.

На первоначальном этапе обучения и общего понимания сути работы, возникает новая проблема: как мотивировать сотрудников-аналитиков и не допустить их ухода из организации. Здесь не существует простого решения, хотя вовлечение аналитиков в решение серьезных вопросов, стоящих перед организацией, и

возможность воочию увидеть результаты своей работы доказали свою эффективность в NÚKIB. Еще одной долгосрочной стратегией является ротация сотрудников при сотрудничестве с CERT вашей организации и другие горизонтальные возможности профессионального роста.


Аналитики в вопросах кибербезопасности из отдела стратегической информации и анализа Национального управления кибернетики и информационной безопасности Чехии (NÚKIB) в главном офисе NÚKIB в г. Брно, Чешская Республика. НАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ КИБЕРНЕТИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Технологии способствуют выполнению миссии

Люди являются наиболее важным достоянием, которое не способны заменить никакие технологии. Именно поэтому правильно выбранные технологии помогают автоматизировать как можно больше процессов, чтобы аналитики с максимальной отдачей могли сосредоточиться на своей работе и исключить любые возможные повторные действия. Однако, у внедрения новых технологий есть определенные пределы. Группа сбора данных и группа аналитиков могут иметь дело лишь с каким-то ограниченным числом инструментов программного обеспечения и максимально использовать их. Именно поэтому в начале процесса планирования следует особенно тщательно выбирать технологии, которые наилучшим образом способствуют выполнению поставленной задачи. Особенно важно, чтобы основные компоненты аналитического программного обеспечения были теми инструментами, которые помогают сотрудникам-аналитикам, а не перегружают их мозг своей сложностью. В группе по сбору данных будут сотрудники с техническим образованием и ученые, специализирующиеся на обработке данных. Крайне важно, чтобы они понимали основную задачу подразделения и нужды сотрудников-аналитиков.

## В поисках одаренных людей

С момента своего основания аналитическое подразделение NÚKIB проводит мероприятия по привлечению к своей работе и к работе агентства в целом новых одаренных сотрудников. В отличие от некоторых других ведомств из сферы безопасности, NÚKIB может и должен находиться на виду. В числе проводимых мероприятий лекции в университетах, организация программ по безопасности и кибербезопасности в «мозговых трестах» и других институтах, а также выступления на конференциях.

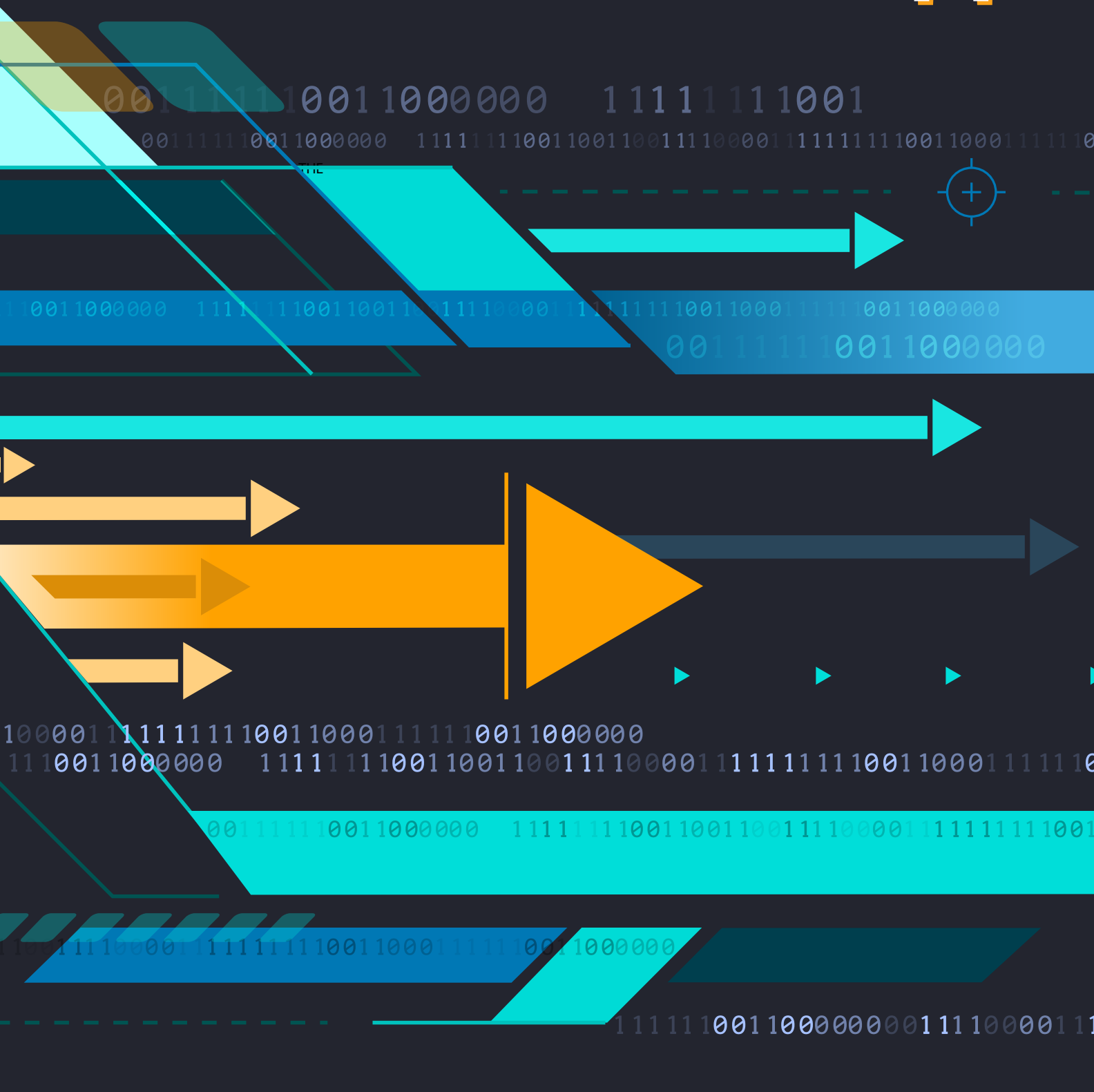
Это подразделение сотрудничает с программой исследования вопросов безопасности в Университете им. Масарика в г. Брно в Чехии, из которой поступило довольно много заявок на программу интернатуры и вакантные должности в NÚKIB. Программа интернатуры оказалась отличной возможностью для ознакомления с профессией студентов, планирующих работать в правительственных органах, а также хорошим способом на практике протестировать потенциальных будущих сотрудников нашего подразделения.

## Заключение

Учитывая направления международного развития и существующие инициативы, такие как Инструментарий ЕС по безопасности 5G или Пражская инициатива, важность нетехнического аспекта кибербезопасности и контекстуализации киберугроз в последующие годы будет только возрастать. Если институты национального уровня, отвечающие за кибербезопасность, планируют эффективно работать без привлечения помощи со стороны, то они должны создать свои собственные аналитические возможности. NÚKIB уже более четырех лет развивает такие возможности, чтобы поддерживать рабочий цикл агентства и снабжать аналитическими материалами руководящих работников в правительственных учреждениях и других институтах стратегической важности.

К созданию аналитического подразделения необходимо относиться как к проекту, требующему долгосрочной целеустремленности как со стороны сотрудников, так и со стороны руководства организации. Группы аналитиков и группы сбора данных являются основным достоянием такого подразделения. Очень редко кандидаты на аналитические должности обладают полным набором всех необходимых навыков и знаний, и поэтому отбирают сотрудников, обладающих ключевыми навыками, к которым позже прибавляются дополнительные. Именно такие супергерои аналитической работы и поддерживают развитие как технических, так и нетехнических аспектов кибербезопасности. □

# ОПТИМАЛЬНЫЙ ПУТЬ ВПЕРЕД



# Эффективный способ создания региональных кадров в сфере кибербезопасности

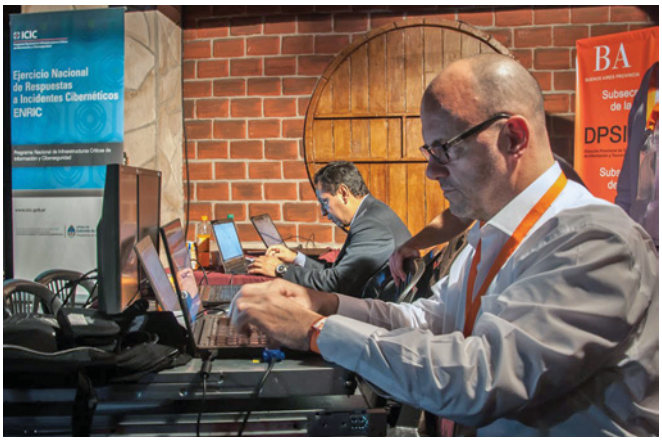
**Педро Джэнисес,** координатор академической деятельности Фонда CAPA 8; **Мариана Галан,** юрисконсульт Управления киберпреступности Министерства безопасности Аргентины и член Комиссии общественной политики, прав человека и конфиденциальности цифровых операций при Фонде CAPA 8; **Максимилиано Скаримболо,** начальник управления полиции г. Буэнос-Айрес; и **Августин Мальпеде,** юрист в Университете Буэнос-Айреса, специализирующийся на информационном праве

ФОТОГРАФИИ НИКОЛАСА ЛОПЕ ДЕ БАРРИОСА

Пандемия COVID-19 в начале 2020 г. привела в некоторых странах к острой необходимости принять меры социальной изоляции и стимулировать дистанционную работу на дому, что заставило частные компании и правительства задействовать все имеющиеся в их распоряжении цифровые инструменты для повышения собственной доступности. Организации, в которых цифровая инфраструктура была минимальной или вообще отсутствовала, были вынуждены за короткое время приобрести и разместить новые цифровые ресурсы, обучаясь их использованию на ходу.

Результатом пандемии стало состояние повышенной гиперподключенности. К этому привел целый ряд факторов, таких как продолжение функционирования компаний, производящих и реализующих товары и предоставляющих услуги, увеличение свободного времени у людей и установление между ними виртуальных отношений, в результате чего они перегружают себя информацией, что вызвало необходимость в многодисциплинарных группах специалистов по вопросам кибербезопасности, занимающихся предотвращением преступлений и обеспечением безопасности.

Эта ситуация также обозначила важность инфраструктуры защиты важной информации, продемонстрировав, что кибербезопасность нужна не только государственному сектору и частным компаниям, но и всем, кто обслуживает и использует компьютерные сети или участвует в обеспечении их функционирования. Все это свидетельствует о настоятельной необходимости увеличения количества профессионалов в сфере кибербезопасности, что позволит странам принять такие последовательные меры как обучение персонала, повышение информированности общественности в вопросах кибербезопасности, принятие необходимых законов для создания прочных юридических рамок и предложение ввести новые общественные правила, регулирующие вопросы кибербезопасности. Это нелегкая задача, поскольку она требует сотрудничества всех вовлеченных субъектов, которые каждый на своем месте должны вносить посильный вклад в создание трудовых ресурсов в сфере кибербезопасности.





Хотя некоторые страны Латинской Америки и Карибского бассейна проявили интерес к организации обучения и проведению киберучений с целью дальнейшего развития своих возможностей, многое все еще предстоит сделать для консолидации экосистемы, охватывающей различные секторы, что позволит принять необходимые меры на региональном уровне.

С точки зрения культуры и общественных отношений, создание региональных трудовых ресурсов в сфере кибербезопасности должно основываться на ценностях, практической деятельности и подходах и традициях отдельных пользователей, экспертов и других субъектов экосистемы кибербезопасности. Социальная и культурная перспектива зависит от роли и функций конкретных субъектов внутри этой экосистемы. Экономические факторы также оказывают существенное влияние на эффективность мер в отношении кибербезопасности.

## ПРАВООХРАНИТЕЛЬНАЯ СИСТЕМА

В правоохранительной системе сотрудники постоянно проходят обучение по вопросам кибербезопасности, хотя деятельность основной их части сосредоточена непосредственно на вопросах киберпреступлений и кибертерроризма. В эти мероприятия вовлечены как правительственные, так и неправительственные организации (НПО), предоставляя широкий круг инструкторов из стран Латинской Америки и других регионов мира.

Правоохранительные органы стран региона полностью задействованы в расследовании международных преступлений, сотрудничая со своими региональными и международными партнерами. Однако, в ряде латиноамериканских стран в связи с особенностями их механизмов проведения расследований правоохранительные органы не имеют всех институциональных возможностей, которые требуются для расследования и обработки случаев киберпреступлений и других нарушений в цифровом пространстве. В этих странах это является прерогативой судебной системы, что зачастую приводит к бюрократическим проволочкам и задержкам в расследованиях.

Неформальное обучение, встречи и семинары оказались полезными для укрепления региональной интеграции и сотрудничества между многочисленными ведомствами, и способствовали созданию сети неофициальных контактов и каналов сотрудничества. На данном этапе правоохранительным органам необходимо формализовать эти контакты и связи и перейти к более плановой и профессиональной системе обучения.

Правоохранительные ведомства должны грамотно подойти к организации мониторинга и помощи этому постепенному переходу на профессиональную основу, создавая технические и оперативные межведомственные протоколы и обеспечивая необходимое обучение на каждом уровне, что повысит стандарты и даст больше возможностей персоналу в сфере кибербезопасности.

Что особенно важно, региональная интеграция между правоохранительными органами в сфере обучения и расширения возможностей приведет к созданию прочной базы трудовых ресурсов, которые будут в состоянии ответить на глобальные вызовы в киберпространстве.

Например, Аргентина в период с 2011 г. по 2015 г. проводила национальные учения, на которых отрабатывались ответные меры в случае киберинцидента. На этих учениях проходила подготовку рабочая группа из 30 человек, состоящая их представителей федеральных правоохранительных сил (Федеральной полиции, береговой охраны, жандармерии и полицейских сил безопасности аэропортов), Вооруженных сил, адвокатов, прокуроров, судей, технических специалистов из частных компаний и правительственных чиновников. Эти учения, которые начались под эгидой Межамериканского комитета по борьбе с терроризмом Организации американских государств (ОАГ), дали импульс совместной работе и развитию специфических возможностей в отношении знания местных законов и культурных особенностей. Несмотря на эти конструктивные усилия, смена правительства в Аргентине привела к власти администрацию с иным подходом к проведению учений, которые в 2016 г. прекратились.

## ЧАСТНЫЙ СЕКТОР

Несмотря на прилагаемые усилия, страны Латинской Америки все еще остро нуждаются в специалистах. По данным «Отчета о состоянии кибербезопасности в 2018-2019 гг.», подготовленного «VU Labs» – компанией,

Участники национальных учений «Ответы на киберинциденты», 14 мая 2015 г., город Мар дель Плат, провинция Буэнос-Айрес, Аргентина.

занимающейся предотвращением мошенничества и защитой частной информации, за последние три года 45,3% участвующих организаций из различных стран стали жертвами кибернападений. Другая публикация на эту же тему, «Доклад об угрозах безопасности сети Интернет – 2018 г.», подготовленная компанией «Symantec», ставит Аргентину на восьмое место среди стран, с территории которых осуществляются кибернападения. А подготовленный в 2016 г. совместный доклад ОАГ и Межамериканского банка развития (МАБР) под названием «Кибербезопасность: мы готовы к ней в Латинской Америке и в Карибском бассейне?» указывает, что хотя регион и набирает обороты в вопросах обеспечения кибербезопасности, региональные возможности все еще очень ограничены по сравнению с нашими европейскими партнерами.

В Латинской Америке местные отделения многонациональных корпораций, в отличие от их головных офисов, не особенно стремятся повышать информированность сотрудников в вопросах кибербезопасности. В результате они не могут создать достаточное количество кадров в сфере кибербезопасности, способных противостоять многочисленным вызовам киберпространства. В этом контексте основополагающую роль будет играть академический сектор . В настоящее время тематику, относящуюся к аспектам кибербезопасности, можно обнаружить только в среде университетских ученых и на аспирантских курсах (да и то с трудом), что существенно ограничивает возможности формирования кадров, знакомых с проблемами в киберпространстве и готовых им противостоять.

Для преодоления этих препятствий страны Латинской Америки должны установить четкие и прозрачные правила и заложить основу для прочной юридической базы, предприняв следующие шаги:

- Поддержка и развитие национальной кибериндустрии, субъекты которой в состоянии понять местные культурные особенности и определить нужды каждой страны региона в сфере кибербезопасности. Это делается, например, путем создания эффективных налоговых стимулов для субъектов, которые инвестируют в развитие и поддержку информационных и коммуникационных технологий (ИКТ).
- Укрепление сотрудничества между общественным и частным сектором с привлечением национальных и международных ИКТ-компаний, а также представителей академической сферы и гражданского общества. Это поможет установить связи между секторами и приведет к формированию широкого цельного видения состояния дел в регионе.
- Укрепление общественного доверия к национальной цифровой инфраструктуре, развитие сотрудничества во всех секторах и привлечение всех граждан к процессу принятия решений.
- Расширение традиционного инструментария в сфере образования на всех академических уровнях, способствование выработке у граждан новой модели поведения, основанной на полном осознании всех опасностей, существующих в киберпространстве.

Повышение уровня ответственности отделений многонациональных корпораций в нашем регионе, кроме других положительных сторон, также позволит принять стандарты защиты в этой сфере, определить правила безопасности и внедрить новые методологии. Это повысит информированность относительно рисков безопасности и понимание необходимости подготовки кадров, отвечающих за эту безопасность, в результате чего появятся возможности обмена знаниями и опытом. Частный сектор должен осознать необходимость использования стандартов, специально предназначенных для сферы кибербезопасности, и соблюдать установленные юридические рамки, сопутствующие процессу.

## ОБЩЕСТВЕННЫЙ СЕКТОР

Как указано в докладе «Индекс глобальной кибербезопасности – 2018», подготовленном Международным союзом электросвязи ООН, в последние годы уровень


Национальные учения «Ответы на киберинциденты», проведенные 20 мая 2014 г. в порту Буэнос-Айреса, Аргентина.

информированности работников общественного сектора региона относительно необходимости разработки стратегий в сфере кибербезопасности возрос и достиг среднего уровня приверженности. В то время как некоторые латиноамериканские страны находятся в процессе разработки собственных стратегий, другие, такие как Аргентина, Чили, Колумбия, Мексика, Парагвай и Перу, такие стратегии уже приняли. При выработке долгосрочных общественных правил и юридических рамок должен приниматься во внимание этот основополагающий документ. Уровень совершенства этих стратегий разный, в том числе и в таком аспекте как создание условий для сотрудничества между правительственными ведомствами, компаниями-операторами объектов критически важной инфраструктуры и частным сектором.

У стран Латинской Америки различные подходы, приоритеты и позиции в отношении создания кадров в сфере кибербезопасности. Хотя общественный сектор признает необходимость работать над широким кругом вопросов – от управления Интернетом и введения инноваций до оказания общественных услуг и приобретения цифрового оборудования – уровень несанкционированного проникновения в Интернет все еще находится на средней/низкой отметке (в среднем 50%). При определении подходов каждой отдельной страны к решению проблемы формирования кадров значительную роль играют социальные и экономические проблемы. Например, некоторые страны предпочтут основное внимание уделять аспекту конфиденциальности, в то время как другие могут отдать предпочтение военному подходу к этому вопросу.

Разработка прочной юридической основы, новых стандартов и технических правил в регионе продвигается медленно. Как было отмечено выше, только несколько латиноамериканских стран имплементировали собственные стратегии кибербезопасности, и еще меньшее количество стран видят необходимость в этом, а также в обновлении своей цифровой инфраструктуры и расширении возможностей в этой сфере на уровне государственной политики. Международные организации, такие как ОАГ и МАБР, оказывают постоянную поддержку в повышении общественной информированности и расширении возможностей в сфере кибербезопасности. Они также призывают страны присоединиться к различным международным инициативам, таким как Глобальный форум по киберзнаниям и Форум по управлению Интернетом.

Некоторые латиноамериканцы не до конца понимают все риски и слабые места, имеющиеся в сфере ИКТ. Это обстоятельство вынудило страны региона предпринять долговременные усилия по обучению национальных кадров и выработке у них чувствительности к этому вопросу, и даже присоединиться к международным кампаниям, нацеленным на создание обществ, осведомленных о проблемах кибербезопасности и решающих эти проблемы.

В случае киберинцидента по официальным каналам проходит ограниченное количество информации. По неофициальным каналам, с другой стороны, можно узнать гораздо больше. Похоже, что на официальные каналы очень сильно влияют такие факторы как боязнь официально подать жалобу, неэффективный механизм подачи жалоб, отсутствие достаточно квалифицированных органов, способных рассмотреть такие жалобы, а также трудности принятия не только мер реагирования, но и превентивных мер.

Все это тесно связано с созданием законодательной базы, нацеленной на предотвращение киберпреступлений. Большинство стран региона осознают, что эти преступления носят международный характер, и это за последние годы привело к расширению регионального сотрудничества. Аргентина, Чили, Колумбия, Коста Рика, Доминиканская Республика, Панама, Парагвай и Перу уже присоединились к международной Будапештской конвенции, регулирующей сферу киберпреступлений. Также в ряде межправительственных органов проводится работа по поиску новых инструментов сотрудничества, при котором более многочисленная группа разнородных стран могла бы обсуждать случаи киберпреступлений и разрабатывать механизм

сотрудничества с учетом региональной асимметрии. Однако, процент наказания за киберпреступления очень низок, судебная система не имеет в своем распоряжении достаточно инструментов для уголовных расследований, а обучение в этой сфере проводится довольно редко.

## НПО И ГРАЖДАНСКОЕ ОБЩЕСТВО

В странах Латинской Америки, особенно в Аргентине, неправительственные организации играют очень важную роль. Они сотрудничают с правительством и вносят свой вклад в визуализацию, понимание и даже совершенствование общественной политики. Вот почему так необходимо принимать во внимание мнение каждого вовлеченного субъекта и работать над созданием прочной законодательной базы, регулирующей такие аспекты как конфиденциальность, права человека и увеличение технических и юридических ресурсов.

НПО также являются важной платформой для свободного выражения мнений и идей, и каждое государство должно использовать это при выработке прочных и жизнестойких правил. Соответственно, резолюция ООН (A/RES/73/27), принятая 5 декабря 2018 г., одобрила такую форму государственной поддержки: «Государства должны содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в укреплении безопасности при использовании ИКТ и самих ИКТ, включая безопасность всей системы производства и сбыта информационных товаров и информационно-технических услуг. Государства должны сотрудничать с частным сектором и организациями гражданского общества в области внедрения правил ответственного поведения в информационном пространстве с учетом их потенциальной роли».

Наглядным примером этого являются семинары и конгрессы, на которые «Fundación CAPA 8», базирующаяся в Аргентине некоммерческая организация, изучающая инициативы в области кибернетики и защищающая их с позиции прав человека, приглашает госслужащих исполнительной, законодательной и судебной власти, а также представителей правоохранительных органов и вооруженных сил. Частный сектор, академические круги и пресса также принимают участие и делятся своими знаниями и мнениями, обеспечивая здоровое обсуждение успехов, ошибок и проблем, с которыми сталкивается Аргентина в своей борьбе с киберпреступлениями.

## ЗАКЛЮЧЕНИЕ

В исследовании «Глобальные трудовые ресурсы в сфере информационной безопасности», проведенном в 2017 г. Центром кибербезопасности и образования и охватившем 170 стран, сделан вывод, что в настоящее время в организациях не хватает специалистов в сфере кибербезопасности, чтобы справляться со всеми нынешними проблемами, и что к 2022 г. глобальный дефицит работников в этой сфере будет составлять 1,8 млн. Тем работникам, которые будут защищать киберпространство страны, требуются знания, а также начальное и последующее профессиональное обучение, которое позволит им адекватно реагировать на растущие количество и изощренность кибернападений. Необходимые курсы обучения в институтах правоохранительных органов (Федеральной полиции, береговой охраны, жандармерии и полицейских сил безопасности аэропортов) должны быть рассчитаны как минимум на два года.

Для этого необходимо выработать государственную политику в вопросах кибербезопасности, которая в дальнейшем будет развиваться благодаря участию различных субъектов кибернетической экосистемы: общественного и частного сектора, академических кругов и НПО.

Сотрудничество и взаимодействие между странами перестало быть простым актом дипломатии; теперь речь идет о выживании и жизнестойкости компьютерных систем всех стран региона. До сегодняшнего дня прогресс в странах Латинской Америки в этой сфере, в большинстве случаев, был результатом усилий, которые также выявили слабые места тех стран, которые еще не встали на этот путь.

«Новая норма» придет к нам в виде гиперсвязей между правительствами, частными компаниями и гражданами, а специализированные группы дипломатов, юристов и технических экспертов будут отвечать на угрозы. Успеем ли мы? Сможем ли мы выровнять региональную асимметрию? Ответ можем дать только мы сами. □

# СОВМЕСТНЫЙ ПОДХОД

## *Стратегия Сербии в образовании, обучении и подготовке трудовых резервов в сфере кибербезопасности*

**Елика Вуядинович** и **д-р Марко Крстич**
Национальная группа реагирования на чрезвычайные компьютерные ситуации Сербии

Значительные усилия правительства Сербии по внедрению цифровых технологий создали условия для роста эффективности и прозрачности системы общественных услуг, но при этом привели к уязвимости страны к кибернападениям. Недостаточное внимание к этой проблеме может снизить благосостояние общества в результате уничтожения экономических достижений и дезорганизации системы услуг, жизненно необходимых для ежедневного функционирования общества, например, производства и снабжения электроэнергией.

Поскольку формальное образование в сфере кибербезопасности находится пока на стадии становления – в настоящее время имеется всего лишь несколько программ магистратуры – правительство, стремясь восполнить этот недостаток, назначило Национальную группу реагирования на чрезвычайные компьютерные ситуации Сербии (SRB-CERT) в качестве органа, ответственного за организацию неформального обучения операторов объектов критически важной инфраструктуры. SRB-CERT уже имеет определенный опыт образовательной деятельности; один из ее членов участвовал в разработке курса по кибербезопасности и в настоящее время является лектором по индустрии информационных технологий на курсе «Магистр 4.0 – Применение передовых информационных технологий в цифровых трансформациях», который читает группа кафедр высших учебных заведений.

### Образовательная стратегия

Принятая SRB-CERT стратегия сочетает два принципа: действуй быстро и используй превентивный подход к возникающим угрозам. В 2019 г. были приняты новые поправки к Закону «Об информационной безопасности», предписывающие Министерству торговли, туризма и

Участники семинара для сотрудников местных органов управления в г. Крагуевац слушают выступления экспертной группы. Октябрь 2019 г. SRB-CERT

телекоммуникаций создать список операторов объектов критически важной инфраструктуры. Еще до того, как министерство разработало такой список, SRB-CERT начала проводить обучение сотрудников местных органов управления, являющихся заинтересованными сторонами с наименьшим объемом инфраструктуры в плане специфических информационных и коммуникационных технологий. Установлению связей и сотрудничеству с местными органами управления способствовал Национальный совет местного экономического развития. Сотрудничество и обмен информацией получили дальнейшее развитие благодаря партнерству общественного и частного секторов, в частности, с компанией «Microsoft», выбранной потому, что она является основным поставщиком операционных систем для местных органов управления.

Искусственный интеллект был признан в качестве зарождающегося технологического направления, которое может значительно повысить выгоды от использования цифровых платформ, но при этом создает новые возможности для организации кибератак. Чтобы подготовиться к будущим проблемам «электронного правительства», SRB-CERT начала анализировать последствия внедрения технологий искусственного интеллекта для возможной картины угроз. В то же время сформированная правительством рабочая группа работала над проектом «Стратегия разработки искусственного интеллекта в Республике Сербия в 2020-2025 гг.», и для нее было очень важно рассмотреть аспект безопасности, связанный с технологиями искусственного интеллекта. Сотрудники SRB-CERT выбрали самое подходящее время для представления результатов своих исследований в вопросе возможного влияния технологий искусственного интеллекта на кибербезопасность – проведение в 2019 г. в Белграде Международного форума по телекоммуникациям.

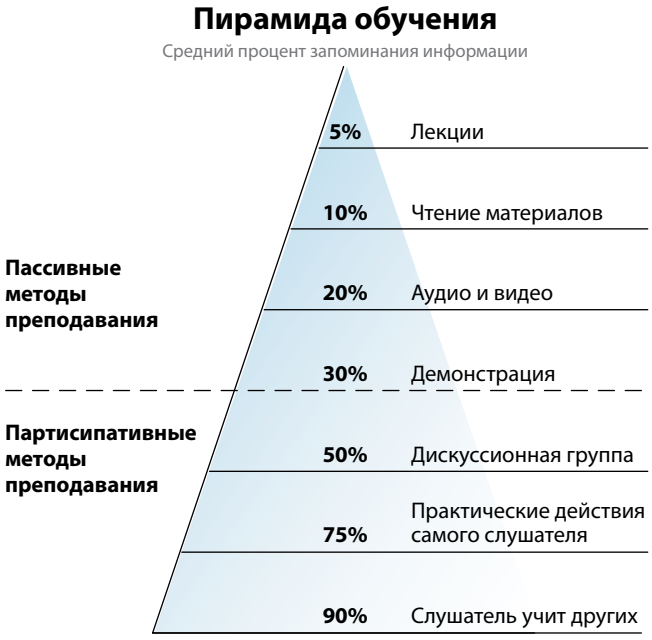
## Образовательные мероприятия для местных органов управления

В обучении сотрудников местных органов управления присутствовал юридический компонент, рассчитанный на управленцев и технический персонал, и технический компонент для системных администраторов. Юридический компонент был посвящен теоретическим и практическим аспектам. У участников была возможность более детально ознакомиться с концепцией «конфиденциальность-целостность-доступность», с существующими сегодня угрозами, с примерами инцидентов в сфере кибербезопасности, с мерами, принимаемыми в сфере безопасности, с моделью «планируй-делай-проверяй-реагируй», а также с Законом «Об информационной безопасности». Практическая часть была сосредоточена на модели Закона «О кибербезопасности», разработанной SRB-CERT для помощи операторам объектов критической инфраструктуры в представлении этого документа, что в соответствии с законодательством является обязательным для их организаций. В ходе учебного курса у слушателей была возможность написать процедуру принятия одной из 28 мер безопасности, заимствованных Законом «Об информационной безопасности» из группы 27000 стандартов ISO/IEC (объединенного технического комитета Международной организации по стандартизации и Международной электротехнической комиссии) и описанных в модели Закона «О кибербезопасности».

Системные администраторы местных органов управления узнали о наиболее распространенных типах нападений в среде Windows, о протоколах аутентификации, о возможностях кражи учетных данных и о подходе системной защиты, предложенном экспертами «Microsoft» в ряде теоретических презентаций и практических упражнений с использованием Системы моделирования кибератак, созданной специально для этих целей.

Были отобраны концепции обучения, сочетающие пассивные и активные методы преподавания в пирамиде обучения. Слушатели могли посещать лекции, читать материалы, пользоваться аудио- и видеоконтентом, присутствовать при наглядной демонстрации и принимать участие в обсуждениях и практической работе. Более того, поскольку сотрудники SRB-CERT участвовали в преподавании на ротационной основе, то все они имели возможность побывать в роли работников образования, что дало им возможность повысить уровень своих знаний.

Особое внимание уделялось аспектам стандартизации, что соответствовало усилиям Глобального форума по киберзнаниям по адаптированию и принятию в Европе американской инфраструктуры трудовых ресурсов, разработанной Национальной образовательной




Источник: использовались материалы из Национальных учебных лабораторий, г. Бетел, штат Мэн, США

инициативой в сфере кибербезопасности (NICE). Технический компонент обучения включал в себя важные знания, навыки и способности, которыми должны обладать системный администратор, аналитик киберзащиты, аналитик безопасности системы, сотрудник, реагирующий на инцидент в сфере киберзащиты, и специалист, оценивающий уязвимость системы. В результате этого учебного курса слушателям были привиты следующие знания, навыки и способности:

**Знания в сфере:**

- Принципов кибербезопасности и конфиденциальности.
- Киберугроз и уязвимых мест.
- Особых оперативных последствий сбоев в системе обеспечения кибербезопасности.
- Организационных правил безопасности для пользователя информационных технологий.
- Методов укрепления системного администрирования, сетей и операционных систем.
- Уязвимых мест приложений.
- Возможностей, ограничений и вклада криптологии в кибероперации.
- Имеющихся сегодня программ и методологий организации активной обороны и укрепления систем.
- Методов и приемов обнаружения деятельности злоумышленников.

**Навыки в сфере:**

- Поддержки функционирования службы каталогов.
- Извлечения информации из захваченных пакетов данных.
- Проверки целостности всех файлов.

**Способности:**

- Применять принципы обеспечения кибербезопасности и конфиденциальности к требованиям конкретной организации.
- Следить за работой системы и реагировать на сигналы аномалии и/или на наблюдаемые подозрительные тенденции или необычную работу системы.

В тренинге, организованном SRB-CERT, приняли участие почти 200 сотрудников из 79 местных органов управления. Доступ к этому тренингу обеспечивался во всех регионах Сербии: в Центральном и Западном регионе, в Южном и Восточном регионе, в Северном регионе и в Белградском регионе. После окончания каждой сессии среди слушателей проводился опрос, позволявший определить степень их удовлетворенности, а также те фрагменты учебного курса, которые нуждались в усовершенствовании.

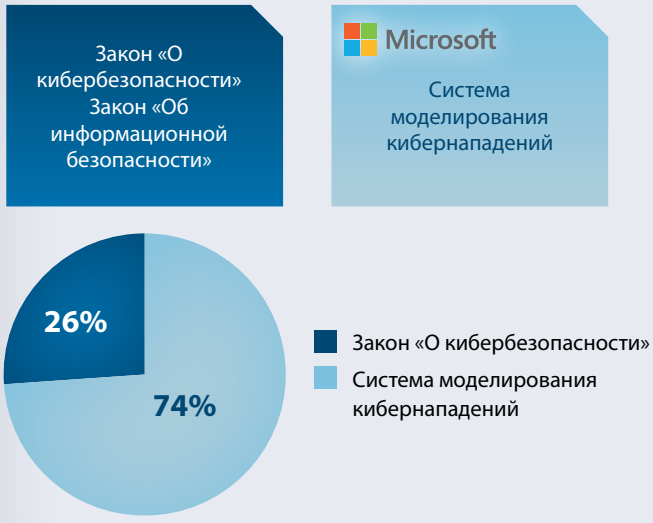
## Будущие угрозы, исходящие от искусственного интеллекта

Возможные угрозы, связанные с искусственным интеллектом, были проанализированы путем использования возможного «обучения машин» в деятельности CERT. Эта тема была выбрана по трем причинам:

- Проинформировать академическую аудиторию о функциях и задачах сотрудников CERT, отвечающих за кибербезопасность.
- Объяснить, как «обучение машин» может повысить эффективность работы CERT.
- Повысить информированность аудитории об аспектах безопасности, связанных с технологиями искусственного интеллекта.

И хотя в центре внимания по-прежнему остается развитие программ специализированного обучения, эта презентация выявила важные факты, касающиеся дальнейшего наращивания трудовых ресурсов в сфере кибербезопасности. Потенциал использования «обучения машин» в механизме оказания услуг CERT стал очевиден, включая потенциал в сфере распространения информации, относящейся к вопросам безопасности, реагирования на инциденты, анализа вирусных программ и проведения киберучений. Однако, использование этих технологий сопряжено с риском. Хотя Национальный институт стандартов и технологий все еще работает над систематизацией возможных типов нападений, связанных с «обучением машин», необходимо отметить, что не у всех видов нападений одинаковая степень вероятности и не все они приводят к одним и тем же последствиям. Это означает, что во время анализа угроз нужно рассматривать модели реалистичных возможностей злоумышленников, и что рабочий цикл создания безопасного программного обеспечения должен включать сканирование

## Семинары | Технические тренинги




Источник: использовались материалы из Национальных учебных лабораторий, г. Бетел, штат Мэн, США

**Количество слушателей по регионам**


Источник: SRB-CERT

уязвимых мест и усиление модели.

И хотя пока что нынешняя версия инфраструктуры NICE признает теорию и принципы «обучения машин» только как важный аспект в обязанностях аналитика данных, оно обладает гораздо большим потенциалом и может трансформировать рабочие обязанности многих других сотрудников.

Позитивное влияние презентации трудно переоценить, и Стратегия развития искусственного интеллекта, принятая спустя несколько месяцев, должным образом учитывает аспекты безопасности.

## Заключение

Сербия является единственной страной в Юго-Восточной Европе, принявшей стандартизационный подход к созданию учебных программ и разработке Стратегии развития искусственного интеллекта, предоставляя другим странам уникальную возможность использовать опыт Сербии и достигнутые ею результаты.

Организованный SRB-CERT тренинг для сотрудников местных органов управления привел к укреплению доверия, повышению степени информированности о киберугрозах и улучшению качества знаний. В результате местные органы управления теперь сообщают о большем количестве киберинцидентов. Этот процесс также позволил определить области, которые необходимо усовершенствовать в последующих обучающих курсах. Знания, навыки и способности членов SRB-CERT были значительно расширены, и было получено подтверждение того, что разработанная SRB-CERT модель Закона «О кибербезопасности» может быть применена и адаптирована к особенностям любой организации-участницы. Хотя о результатах стандартизации обучения говорить еще рано, ожидается, что более точная информация о рабочих обязанностях и требованиях к обучению будет подготовлена к началу следующей фазы обучения. В центре следующего этапа обучения будет организация более продвинутого уровня образования для сотрудников местных органов управления, а для другой группы операторов объектов критически важной инфраструктуры будет использоваться та же самая методология и базовый уровень преподавания.

Первый шаг в создании обучающих программ по вопросам безопасности, связанным с искусственным интеллектом, уже был сделан. Необходимо провести дополнительные исследования для того, чтобы окончательно определиться с учебным планом, целевой аудиторией и методами обучения. Исследование, проведенное недавно Институтом «Будущее человечества» при Оксфордском университете в Великобритании, показало, что научный анализ соотношения нападение-оборона технологий искусственного интеллекта отличается от анализа уровня компьютерной безопасности, поскольку существует гораздо большая вероятность обнаружения методов, которые злоумышленники сами не откроют, но смогут использовать в своих интересах во время нападений. Поэтому рекомендуется обсуждать оборонительные и наступательные аспекты вместе и избегать предоставления информации о нападениях, содержащих трудно исправимые социальные компоненты, соблюдая при этом особую осторожность в ситуациях, когда вы делитесь кодами источников. □

# УСТРАНЯЯ ДЕФИЦИТ КВАЛИФИЦИРОВАННЫХ КАДРОВ

## КАК ФИЛИППИНЫ УДОВЛЕТВОРЯЮТ ПОВЫШЕННЫЙ СПРОС НА ПРОФЕССИОНАЛОВ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

**Геналин Масалинао**, специалист по информационным технологиям, Отдел информационных и коммуникационных технологий Филиппин

Жесткие ограничительные меры привели к застою в национальных экономиках по всему миру, сдерживая распространение вируса, но при этом нанося огромные экономические потери. На Филиппинах подавляющее большинство компаний настойчиво рекомендуют и требуют, чтобы их сотрудники работали из дома из-за пандемии COVID-19, так что не удивительно, что все чаще стали возникать инциденты, связанные с кибербезопасностью и конфиденциальностью данных.

Никогда ранее недостаток профессионалов в сфере кибербезопасности в стране не был так очевиден. И хотя этот вопрос неоднократно поднимался различными субъектами, заинтересованными в укреплении кибербезопасности, только во время нынешней национальной чрезвычайной ситуации все в стране почувствовали острую необходимость создания надежной инфраструктуры кибербезопасности и наличия рабочей силы, способной обеспечить бесперебойную работу правительства и других критически важных объектов инфраструктуры.

Как никогда необходимы кадры в секторе информационных технологий (ИТ), чтобы поддерживать функционирование правительства и важных объектов инфраструктуры, обеспечивать предприятиям выход в Интернет и поддерживать связь между людьми. Специалисты в сфере кибербезопасности играют чрезвычайно важную роль в работе тех, кто предоставляет медицинские услуги, производит технические продукты и компоненты, обеспечивает безопасность и обслуживание центров хранения важных данных, доставляет продукты питания и оказывает жизненно важные услуги населению. Они обеспечивают доступ в Интернет школьникам, которые сейчас обучаются в онлайновом режиме, а также дают возможность правительствам принимать ответные меры в этой кризисной ситуации в сфере здравоохранения.

Наблюдается очень серьезный разрыв между имеющимся в наличии и требуемым количеством квалифицированных работников в сфере кибербезопасности, как раз именно тогда, когда потребность в них особенно велика. Еще до начала пандемии издание «Cybersecurity Ventures» прогнозировало, что к 2021 г. в глобальном масштабе будет 3,5 млн. вакантных должностей, что приведет к кризисной ситуации в этом секторе. В соответствии с данными Международного консорциума по сертификации в области безопасности информационных систем (ISC)², в 2016 г. Филиппины отставали от своих партнеров по Ассоциации стран Юго-Восточной Азии, имея всего 84 сертифицированных специалиста в сфере информационной безопасности (CISSP). У Индонезии было 107 специалистов, у Таиланда 189, у Малайзии 275 и у Сингапура 1 тыс. специалистов. Кроме того, половина из этих 84 филиппинских специалистов работали за пределами страны. Исследование, проведенное в 2018 г. компанией «IBM» и Институтом им. Понемона, показало, что дефицит квалифицированных специалистов в сфере кибербезопасности создает очень рискованную ситуацию, когда количество случаев нападений и изощренных похищений данных растет, и при этом нет компетентных профессионалов, которые могли бы обнаружить и предотвратить эти нападения. Подтверждением тому служит ряд резонансных инцидентов в сфере кибербезопасности и похищения данных, произошедших на Филиппинах один за другим.

Наиболее серьезным случаем было проникновение в компьютерную систему Избирательной комиссии. 27 марта 2016 г. хакеры под лозунгом «Анонимные Филиппины» взломали вебсайт Избирательной комиссии Филиппин и удалили с него информацию. Хакеры оставили послание, призывающее к принятию мер по усилению кибербезопасности считающих голоса аппаратов, которые должны были использоваться на всеобщих выборах на Филиппинах 9 мая 2016 г. Не имея плана

обеспечения кибербезопасности, страна была отдана на милость киберпреступников.

Спустя месяц после выборов законом Республики № 10844 был создан Отдел информационных и коммуникационных технологий (DICT). DICT является правительственным органом, отвечающим за разработку правил и планов развития информационных и коммуникационных технологий (ИКТ) в стране. У него имеются широкие полномочия в сферах телекоммуникаций и вещания, кибербезопасности, конфиденциальности данных, защиты потребителей, а также содействия торговле и инвестициям в ИКТ и услуг, основанных на ИКТ. Отделу едва исполнился год, когда он опубликовал «Национальный план обеспечения кибербезопасности – 2022» (NCSP), который для страны является своеобразной дорожной картой создания на Филиппинах жизнестойкой киберсистемы.

NCSP представляет собой основу для выработки политики в сфере кибербезопасности, в том числе и плана выполнения намеченных задач. Были изложены ключевые стратегические инициативы, содержащие комплексный многоуровневый механизм реагирования с целью более эффективной защиты критически важной инфраструктуры от киберугроз. Ключевым обязательным элементом Национального плана обеспечения кибербезопасности является поддержка развития квалифицированных сотрудников в сфере кибербезопасности. Документ NCSP 2022 определяет следующие основные программные области, направленные на удовлетворение возросшей необходимости улучшения информированности населения и создание новых возможностей в государственном и частном секторах:

- Защита критической информационной инфраструктуры (КИИ) путем оценки кибербезопасности и доведения ее до установленных стандартов, проведения национальных киберучений и тренировок и создания национальной базы данных для мониторинга и отчетности.
- Защита правительственных компьютерных сетей посредством принятия национальной программы реагирования на компьютерные чрезвычайные ситуации, программы развития возможностей и повышения квалификации в этой области, создание резерва экспертов в сфере информационной безопасности и кибербезопасности, Центра операций по выявлению и анализу угроз, защиты правительственных электронных транзакций и обновления лицензионного программного обеспечения.
- Защита системы поставок посредством принятия программы оценки и сертификации национальных общих критериев.
- Защита населения путем ускорения процесса обучения и получения необходимых навыков, запуска проекта пропагандирования необходимости обеспечения кибербезопасности, проведения национального «Месяца информированности населения по вопросам кибербезопасности» и создания для правительства и данной программы возможностей сотрудничества на национальном и международном уровне.

Бюро кибербезопасности DICT проводит «круглые столы» с 12 секторами КИИ (правительство, информационные коммуникации, энергетика, авиация, морские перевозки, наземный транспорт, здравоохранение, банковско-финансовая сфера, водоснабжение, безопасность и чрезвычайные ситуации, средства массовой информации и процесс промышленного аутсорсинга), приглашая академических работников, чтобы они ознакомились с нуждами промышленности. Именно это начинание и проложило путь к партнерству с академическими кругами, которое привело к разработке учебных программ по вопросам кибербезопасности.

Бюро также участвует в работе технической группы Комиссии по высшему образованию (CHED) и способствует разработке правил, стандартов и рекомендаций (PSG) для программы бакалавриата в области кибербезопасности. Второй проект PSG в настоящее время проходит этап консультаций.

Ожидая принятия комиссией CHED правил, стандартов и рекомендаций для программы бакалавриата в области кибербезопасности, DICT постоянно обращается к средним школам с предложением ввести в их учебные программы предметы, связанные с кибербезопасностью.

В настоящее время некоторые институты предлагают новые курсы по тематике кибербезопасности. Это является частью усилий правительства Филиппин по расширению навыков и знаний студентов в сфере наук, технологий, инженерных специальностей и математики. Не удивительно, что, будучи первым учебным заведением на Филиппинах, преподающим курсы по ИТ, Университет AMA также стал первым университетом в стране, предложившим ввести степень бакалавра по предмету кибербезопасности. Это стало возможным благодаря партнерству с Бюро кибербезопасности DICT, а стимулом послужила учебная программа по кибербезопасности, разработанная Европейским центром исследований безопасности им. Джорджа Маршалла. В ответ на потребность в формальном образовании в сфере кибербезопасности, Университет AMA сейчас принимает заявления от абитуриентов в своем основном кампусе в г. Куезон Сити на Филиппинах. А частный сектор выступил с инициативой создания партнерства между фирмой «Palo Alto Networks», специализирующейся на вопросах безопасности, и Азиатско-Тихоокеанским колледжем с целью открыть первую на Филиппинах академию кибербезопасности.

Хотя некоторые учебные заведения на Филиппинах ввели в свои учебные планы предметы, связанные с кибербезопасностью, многое все еще предстоит сделать, чтобы устранить огромный разрыв между нуждами промышленности и нынешней ситуацией с квалифицированными кадрами в сфере кибербезопасности. □

# ЗАЩИЩАЯ МАВРИКИЙ ОТ КИБЕРУГРОЗ

**Национальная Группа реагирования на инциденты в сфере кибербезопасности (G-SIRT) ведет постоянную борьбу за наращивание возможностей киберзащиты**

**Мадан Кумар Мулхе**
Отдел безопасности информационных технологий, Министерство информационных технологий, коммуникаций и инноваций Маврикия

Последние три выпуска Глобального индекса кибербезопасности (GCI), издаваемого Международным союзом электросвязи ООН, назвали Маврикий страной, проявляющей наибольшую заинтересованность в создании системы кибербезопасности на африканском континенте. В этой статье анализируется, как правительственная G-SIRT решает задачу расширения возможностей, одну из пяти основ при оценке GCI.

## Важность развития возможностей

G-SIRT функционирует в составе Отдела безопасности информационных технологий (ITSU) Министерства информационных технологий, коммуникаций и инноваций. ITSU постоянно подчеркивает важность непрерывного повышения квалификации своих технических сотрудников в целях решения следующих задач:

- Реализация правительственной политики в сфере безопасности информационных технологий (ИТ).
- Оказание помощи министерствам и ведомствам по внедрению стандартов безопасности.
- Распространение информации о безопасности ИТ.
- Проведение проверок систем кибербезопасности.
- Реагирование на инциденты в сфере безопасности ИТ.

Уровень информированности госчиновников по вопросам кибербезопасности повышается следующими путями:

- Проведением презентаций на тему безопасности ИТ на местах.
- Распространением материалов с информацией об угрозах, таких как фишинг, вирусы-вымогатели и хищение персональных данных.
- Созданием обучающего модуля по вопросам кибербезопасности, доступного круглосуточно через электронную систему связи.

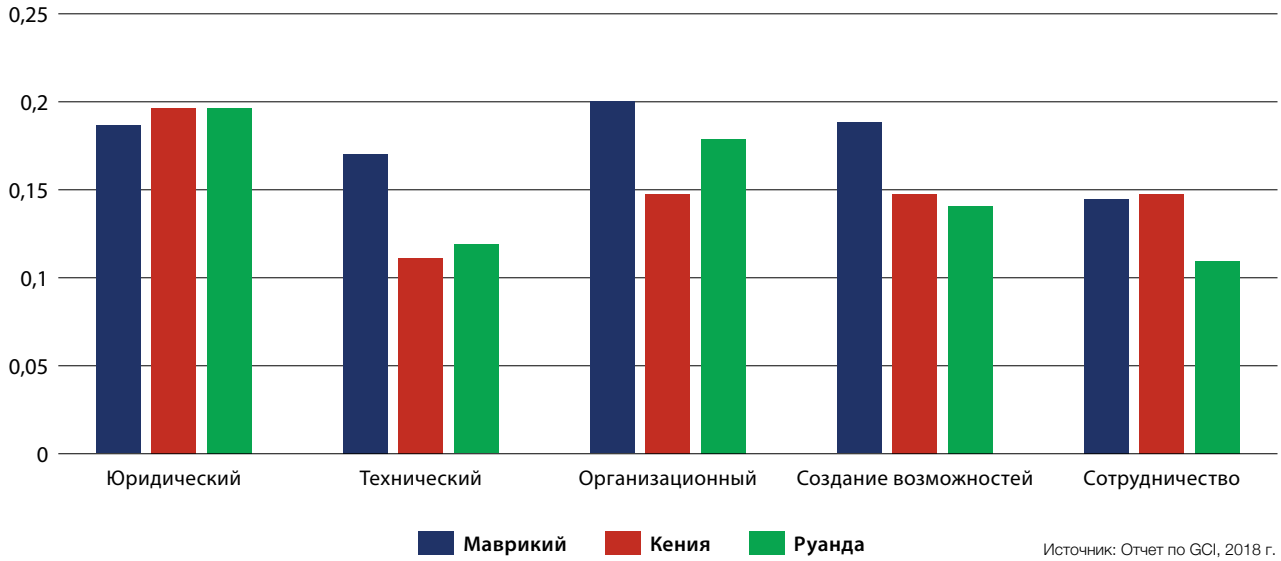
G-SIRT постоянно сотрудничает с национальной Общественной группой реагирования на чрезвычайные ситуации Маврикия (CERTMU), которая реагирует на киберинциденты на национальном уровне. G-SIRT функционирует как группа реагирования на инциденты, происходящие в государственных учреждениях. CERTMU провела несколько обучающих мероприятий и учений по кибербезопасности для субъектов государственного и частного секторов на региональном и международном уровнях.

В последних киберучениях участвовали группы специалистов из правительственных учреждений Маврикия, такие как G-SIRT, центр хранения данных и ИТ-операторы различных министерств и правоохранительных органов. Одной из основных целей учений было привить G-SIRT достаточно знаний и опыта для проведения киберучений для правительственных чиновников в таких ключевых секторах как здравоохранение, энергетика и коммунальные услуги, что является главной задачей на период 2020-2021 гг.

## Управление информационной безопасностью

Основным проектом в Национальной стратегии кибербезопасности Маврикия (NCSS) было принятие международного стандарта информационной безопасности (ISO/IEC 27001) Международной организации стандартизации (ИСО) в государственном и частном секторах. Для государственного сектора ITSU разработал новаторский подход к созданию централизованной инфраструктуры управления информационной безопасностью, основанный на модели управления рисками и согласованный со стандартом. Эта инфраструктура состоит из планов-шаблонов ответов на риски по отдельным угрозам безопасности, общим для всех министерств, которые легко могут быть приспособлены к конкретным нуждам каждого сектора.

### Три наивысших результата в африканском регионе по пяти основным элементам GCI




Источник: Отчет по GCI, 2018 г.

# КРАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ

*'Знай про опасности'*

## Что такое кража персональных данных?

Кража персональных данных происходит тогда, когда злоумышленник использует персональную информацию другого человека, например, его имя, адрес, идентификационный номер, номера кредитной карты или банковского счета, в целях мошенничества. Это может относиться и к организации; в этом случае создается «фейковый» профиль. Кража персональных данных считается наиболее распространенным киберпреступлением в мире.

Мошенники могут получить персональную информацию другого человека следующими способами:

- Использованием Интернета для поиска информации о человеке или организации.
- Кражей бумажника у другого человека.
- Кражей электронной почты другого человека.
- Просмотром содержимого мусорного ведра другого человека (исследованием содержимого мусорных контейнеров).
- Использованием вредоносных компьютерных программ/подделкой сообщений электронной почты.
- Похищением цифровой информации.

**Если у вас есть подозрения, что вы стали жертвой похищения персональных данных, свяжитесь с соответствующими органами – полицией или своим банком.**

## Признаки похищения персональной информации:

- Ваша выписка из банковского счёта содержит покупки, о которых вы ничего не знаете.
- Вы получили кредитные карточки, которые не запрашивали.
- Банк отказался выдать вам кредитную карту без видимых причин.
- От компаний вам поступают звонки или письма о товарах/услугах, которые вы не покупали.
- В Интернете вы находите профиль с вашим именем или именем вашей организации, но вы в этот профиль не можете войти.

## Последствия кражи персональных данных

После кражи у вас персональных данных, их могут использовать для:

- Покупки товаров с использованием вашей кредитной карты или банковского счета.
- Совершения мошенничества от вашего имени.
- Создания «фейковых» профилей от вашего имени
- Подрыва вашей репутации или репутации вашей организации.

## Защита от похищений персональных данных

- Не передавайте свои персональные данные, особенно электронным путем, пока не убедитесь, с кем имеете дело.
- Ни с кем не делитесь своей чувствительной информацией (паролями, персональными идентификационными кодами).
- Для всех своих учетных записей используйте сложные пароли.
- Делайте покупки на безопасных и заслуживающих доверия вебсайтах (https:).
- Никогда не сохраняйте свою личную информацию на компьютерах в общественных местах (например, в интернет-кафе).
- Установите и обновляйте антивирусные программы.
- Не используйте один и тот же пароль для различных учетных записей.
- Соблюдайте осторожность при общении в социальных сетях.
- Соблюдайте правила безопасности во время поиска информации в Интернете.

Источник: Министерство информационных технологий, коммуникаций и инноваций Маврикия

Технические сотрудники прошли обучение по вопросам создания такой структуры; это позволило им стать основными координаторами для министерств и ведомств в ходе внедрения стандартов и соответствующего обучения. Кроме того, при создании специализированных возможностей, международные сертифицирующие органы, такие как индийское Управление тестирования стандартов и сертификации качества, провели обучение специалистов в сфере кибербезопасности нашего министерства по учебным планам изучения стандартов ИСО «по умолчанию». Сотрудники G-SIRT также получили квалификацию аудиторов систем безопасности для внутренних проверок.

## Правительственная группа реагирования на инциденты в сфере кибербезопасности

G-SIRT эффективно реагирует на инциденты в сфере безопасности информационных и коммуникационных технологий (ИКТ), оказывая проактивные и реактивные услуги по борьбе с киберугрозами. Частью реактивных услуг G-SIRT является мониторинг управления инцидентами в государственных службах с использованием автоматизированной системы реагирования на инциденты, включающей в себя базу данных знаний, предоставляемую в распоряжение профессионалов в сфере кибербезопасности и оперативного персонала по ИКТ. Эта интернет-основанная система позволяет проводить автоматическое расширение масштабов инцидента – раньше это делалось вручную – что ускоряет процесс управления инцидентом с более широким обменом необходимыми знаниями. Группа специалистов G-SIRT также обучила оперативные группы ИТ-экспертов, направленных на работу в министерства и ведомства, моделям реагирования на инциденты.

Участие технических сотрудников в семинарах и киберучениях помогает повысить эффективность реагирования на инциденты и расширяет возможности предоставления рекомендаций субъектам в государственном секторе. Взаимодействие между участниками региональных и международных семинаров ускоряет процесс обучения и обмена информацией, и это чрезвычайно важно, поскольку киберугрозы не признают государственных границ.

В соответствии с Законом «О компьютерных злоупотреблениях и киберпреступлениях», все похожие на киберпреступления инциденты направляются на расследование в Отдел киберпреступлений полиции. В случае инцидентов национального масштаба G-SIRT также взаимодействует с национальной CERT.

В сфере проактивных действий наша группа проводит аудиты систем безопасности по всему сектору государственных служб. Однако, учитывая возрастающую сложность и запутанность современных киберугроз, для эффективной защиты правительства потребуются дополнительные инструменты

и соответствующее обучение. Более того, G-SIRT рассматривает возможность расширения круга своих услуг и включения в него анализа вирусных программ и криминологического аспекта, что потребует еще большего наращивания способностей сотрудников.

## Обучение и сертификация

Основная трудность, с которой сталкивается G-SIRT — это необходимость постоянного повышения квалификации персонала и его сертификации, чтобы противостоять непрерывному появлению новых угроз кибербезопасности. Хотя наши технические сотрудники получают большую пользу от участия в практических занятиях и семинарах, на которые их приглашают коллеги из других стран, по мере появления новых технологий, таких как искусственный интеллект и «Интернет вещей», недостаток знаний и навыков продолжает увеличиваться.

Доля сертифицированных сотрудников низка с учетом количества угроз в этой новой сфере. Для того, чтобы группа была лучше подготовлена к реагированию на угрозы, необходимы сертифицированные курсы подготовки в сфере кибербезопасности. Кроме того, для того, чтобы оказывать предполагаемые дополнительные услуги (например, анализ вредоносных программ и аудит систем кибербезопасности), необходимо профессиональное обучение наших сотрудников.

Еще один проект NCSS – введение предмета кибербезопасности в образовательные учебные планы на первичном, вторичном и третичном уровнях. Нет никаких сомнений в том, что знакомство населения с вопросами кибербезопасности будет способствовать наращиванию возможностей наряду с формированием будущих профессионалов для сектора кибербезопасности. G-SIRT может сотрудничать с академическими кругами и, в дополнение к их академическим знаниям, передавать молодым специалистам практические знания и опыт.

## Заключение

G-SIRT и дальше будет делать упор на профессиональное развитие по мере того, как она будет расширять круг своих услуг по борьбе с киберугрозами, тем самым внося свой вклад в укрепление позиций Маврикия в рейтинге GCI. В обстановке постоянного роста количества киберрисков необходима программа расширения профессиональных возможностей сотрудников, чтобы противостоять существующим угрозам и обладать способностью вырабатывать модели реагирования на новые угрозы, порождаемые новыми технологиями. □

# СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (ISMS)

*'Знай про РИСКИ, чтобы лучше ОБЕЗОПАСИТЬ себя'*

### Информационная безопасность

Информация является одним из наиболее ценных активов любой организации и существует во многих формах. Безопасность информации означает защиту информации от широкого круга угроз с целью сохранения ее конфиденциальности, целостности и доступности.

### Система управления информационной безопасностью

ISMS – это инфраструктура управления, основанная на подходе управления рисками, созданная для реализации и совершенствования информационной безопасности. Она позволяет организации:

- Определить потенциальные угрозы и их влияние на бизнес-процессы.
- Оценить степень риска в нескольких областях.
- Принять соответствующие меры для устранения или минимизации этих рисков.

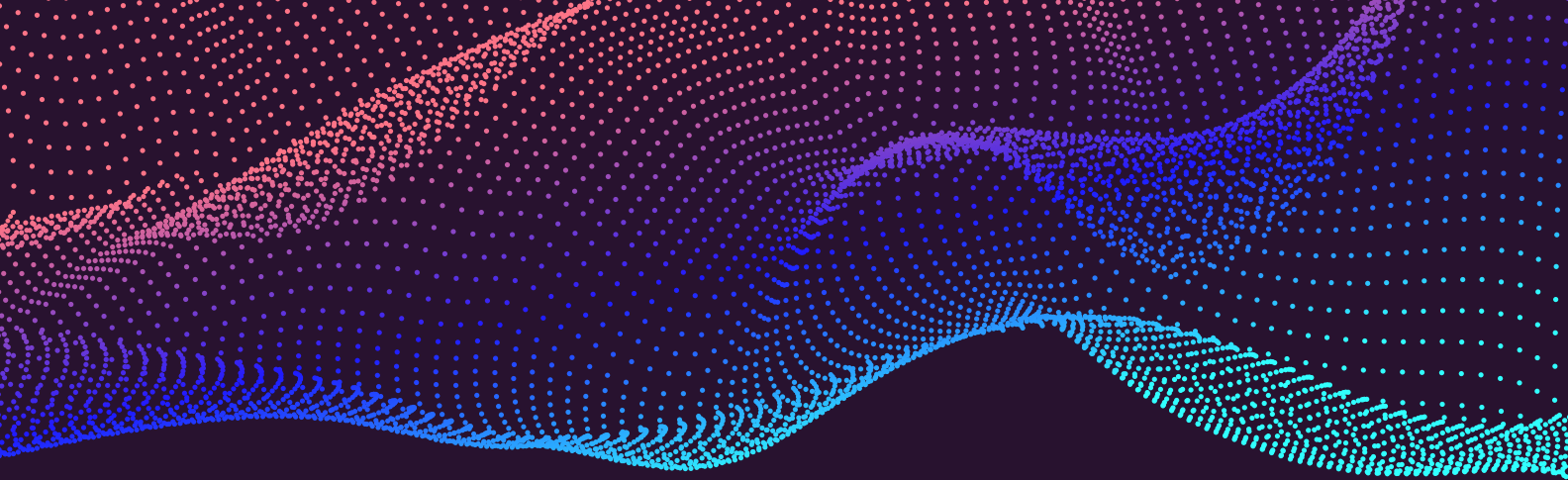
Международный стандарт ISO/IEC 27001 предлагает комплексный набор мер, содержащих передовой опыт в сферах информационной безопасности, управления рисками и контроля за безопасностью.

### Положительный эффект ISMS

- Обеспечение информированности пользователя об угрозах безопасности и необходимых мерах.
- Планирование мер по эффективной защите своей компании.
- Стимулирование эффективного управления рисками.
- Более эффективное реагирование на инциденты в сфере информационной безопасности.
- Повышение уверенности у всех заинтересованных сторон.

### Шаги по внедрению ISMS на основе ISO/IEC 27001

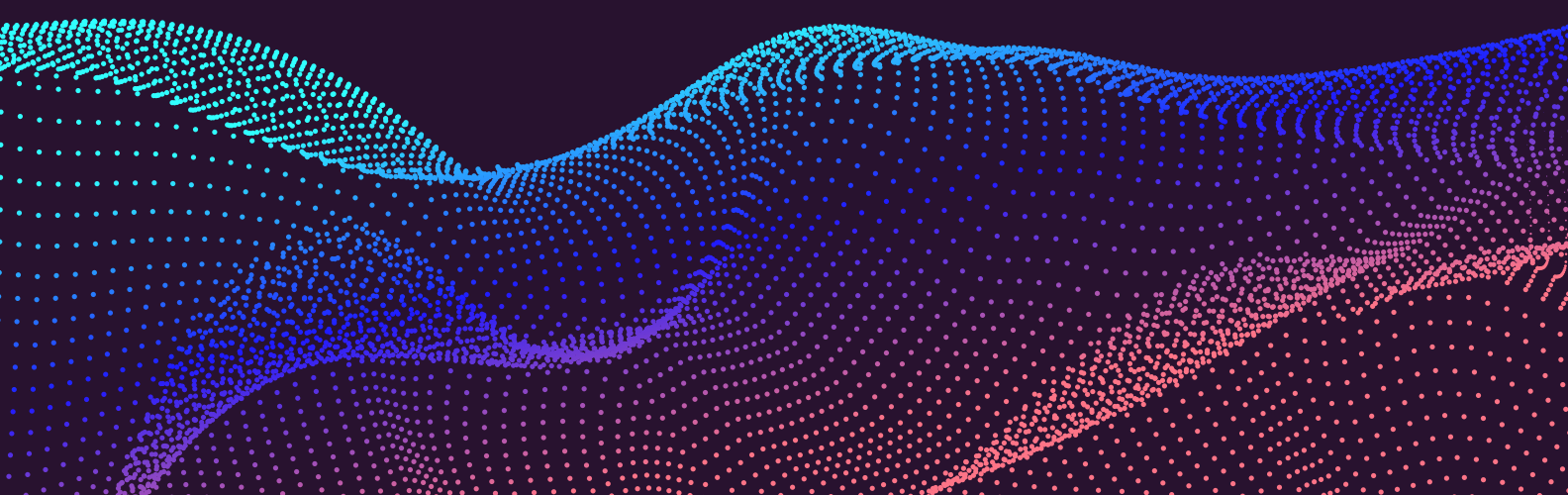

Источник: Министерство информационных технологий, коммуникаций и инноваций Маврикия



# ИДЕАЛЬНОЕ СОЧЕТАНИЕ

## КИБЕРУЧЕНИЯ И НАЦИОНАЛЬНЫЕ ПРАВИЛА И ПРОЦЕДУРЫ

**Вероника Нетолицка** и **Петр Новотны**
Национальное агентство компьютерной и информационной безопасности Чешской Республики



В Чешской Республике киберучения считаются одним из наилучших инструментов укрепления кибербезопасности. Они позволяют проводить моделирование реалистичных кризисных ситуаций в контролируемой обстановке – а разве существует лучший способ обучить и подготовить сотрудников к кризисной ситуации, чем дать им возможность пережить ее в ходе смоделированного сценария? Существует много полезных и нужных инструментов (например, семинары, учебные курсы и конференции), но ни один из них не дает такой возможности реально прочувствовать кризисную ситуацию как киберучения.

Подобно многофункциональному швейцарскому армейскому ножу, учения выполняют множество задач (см. Рисунок 1), что еще больше подтверждает их эффективность. Способность обнаружить и высветить слабые места в национальных правилах и процедурах может быть достигнута на учениях различных видов, таких как технические, теоретические, процедурные и коммуникационные учения. Некоторые учения могут быть специально организованы для проверки и оценки национальных правил и процедур, в то время как для других учений такие проверки и оценки будут всего лишь побочным результатом.

Почему необходимо оценивать эффективность правил и процедур путем проведения учений? Во-первых, потому что некоторые правила и процедуры могут быть уже устаревшими. Возможно, национальные правила и процедуры были приняты задолго до того, как критически важные объекты вступили в киберэпоху. Хорошим примером могут служить юридически закрепленные правила поведения в случае чрезвычайной ситуации. Они уже существуют не одно десятилетие, но пригодятся ли они в случае кризисной ситуации в киберпространстве? Во-вторых, даже если предположить, что существуют обновленные процедуры принятия мер активной обороны, как вы можете убедиться в том, что они будут эффективны и применимы во время кибернападения на объекты критически важной инфраструктуры? Естественно, это хотелось бы знать до того, как возникнет реальная кризисная ситуация. И наконец, кибербезопасность – это динамичная, быстро эволюционирующая сфера.

Правила и процедуры должны обновляться постоянно, и необходимость в новых правилах и процедурах неоспорима. Возьмем хотя бы внедрение сетей 5G: телекоммуникационные сети следующего поколения служат наглядным примером того, как новые технологии создают необходимость в принятии обновленных национальных правил и процедур. Учения могут помочь выявить такую необходимость.

К учениям мы применяем комплексный подход. Приглашаются участники всех уровней (стратегический, оперативный и тактический) и охватываются все соответствующие аспекты (технический, политический, экономический, медийный, юридический, этический и т.д.). Последние несколько десятилетий вопрос кибербезопасности выходил далеко за рамки чисто технической области и напрямую затрагивал политическую, военную, экономическую, юридическую и медийную сферы. Все эти сферы имеют прямое отношение к национальным правилам и процедурам. Если в ходе учений планируется охватить эти аспекты, то необходимо приглашать и соответствующих участников – квалифицированных юристов и экспертов из СМИ, служащих вооружённых сил и особенно людей, отвечающих за принятие решений. Кроме того, желательно вводить в сценарии учений новые и ожидаемые тенденции. Это помогает сделать их эффективным инструментом в решении назревающих проблем.

## Сочетание киберучений и национальных правил и процедур

Как указывалось выше, обнаружение слабых мест на ранних стадиях приносит пользу при составлении и корректировке национальных правил и процедур. Каждые учения должны стремиться отразить самые последние события, уделяя особое внимание подготовленности персонала к реагированию на нападение, что отвечает требованиям хорошо отлаженной и скоординированной системы. Найденные недостатки оцениваются с точки зрения их влияния на функционирование национальной системы обеспечения кибербезопасности. Опыт Чехии показывает, что процесс обнаружения этих слабых мест представляет собой замкнутый круг с исходными данными и получаемыми результатами. Исходные данные поступают из многих источников, например, из результатов предыдущих учений или от их организаторов. Однако, наибольший объем исходных данных поступает от специалистов по национальным правилам и процедурам. Все эти исходные данные

**Рисунок 1**


Источник: Национальное агентство компьютерной и информационной безопасности Чешской Республики

помогают лучше продумывать сценарии учений и сделать их более реалистичными. Получаемые результаты учений должны иметь прямое отношение к вопросам по национальным правилам и процедурам, рассматриваемым на стратегическом уровне. За этот процесс отвечают люди, хорошо знакомые как с существующими правилами и процедурами, так и с особенностями проведения учений – люди, которые могут предоставить исходные данные, подходящие для конкретных учений, и указать те результаты проведенных учений, которые помогут усовершенствовать национальные правила и процедуры.

### Чехия: полученный опыт и извлеченные уроки

В 2016 г. чешскому правительству был представлен первый документ, описывающий слабые места в национальных правилах и процедурах, относящихся к кибербезопасности. Документ был основан на наблюдениях за функционированием системы обеспечения национальной кибербезопасности и содержал анализ наиболее серьезных проблем в действовавшей системе. Полученные в ходе киберучений результаты являются основным источником данных, приведенных в этом документе. Анализируя выявленные слабые места, можно извлечь уроки, благодаря которым можно сделать весь процесс успешным:

- **Развитие трудовых ресурсов** — Основой успешного сотрудничества между инстанцией, отвечающей за национальные правила и процедуры, и организаторами учений, являются люди. Необходимо сделать так, чтобы представители этих двух групп специалистов понимали планы и задачи друг друга и поддерживали постоянную связь. Чем больше исходных данных смогут предоставить те, кто отвечает за правила и процедуры, тем больше ценных результатов смогут им выдать организаторы учений. Давайте специалистам по разработке национальных правил возможность участвовать в учениях или хотя бы присутствовать на них, поскольку если эти специалисты осознают отдельные аспекты киберпространства посредством участия в учениях и поймут технические основы проблемы, то у них будет больше знаний при выработке правил и процедур. Однако, организаторам учений пойдет на пользу, если они сами будут обладать знаниями о соответствующих правилах и процедурах. Давайте им возможность повышать свою квалификацию и поддерживайте их стремление получить образование и знания в областях, не связанных с организацией учений. Такой подход окупится сторицей в будущем.
- **Отбор** — Выбор недостатков, которые затем войдут в список задокументированных слабых мест, должен соответствовать природе национальных правил и процедур и составляться по принципу приоритетности. Когда система далека от завершенности, принцип приоритетности очень важен.
- **Всеправительственный подход** — Национальная система обеспечения кибербезопасности охватывает многие заинтересованные стороны (например, операторов объектов национальной

**Рисунок 2**


Источник: Национальное агентство компьютерной и информационной безопасности Чешской Республики

Во время симпозиума «Устремления Африки» в 2019 г. в Гане проводились нетехнические теоретические учения.
АФРИКАНСКОЕ КОМАНДОВАНИЕ ВС США

критически важной инфраструктуры, регулирующие органы, Интернет-провайдеров и правоохранительные органы). По этой причине все соответствующие организации должны быть включены в процесс обсуждения обнаруженных слабых мест. Кибербезопасность на национальном уровне не может быть обеспечена каким-то одним назначенным органом. В ходе этого процесса должно устанавливаться доверие между участвующими сторонами, что в случае с Чешской Республикой было крайне важно.

- **Систематичность** — В идеале, документ, указывающий на слабые места, должен издаваться регулярно, поскольку во время учений также выявляются новые недостатки. Ежегодные обновления такого документа обеспечат достаточно частое и стабильное представление соответствующей информации.
- **Предложение решения** — Этот продукт должен не только обратить внимание на выявленные недостатки в системе. Также очень важно представлять и варианты решений обнаруженных проблем, основываясь на проведенных обсуждениях с соответствующими субъектами. Такой подход важен для дальнейшей реализации принятых решений. Неудивительно, что учения могут занимать соответствующее место в этом процессе. Когда в ходе учений участники обнаруживают слабое место и порождаемую им проблему, они пытаются тут же найти ее решение. Иногда участники из других стран делятся своим передовым опытом. Это может быть еще одним ценным результатом, включенным в документ, указывающий на недостатки в существующей системе.
- **Постоянная оценка** — Оценка должна проводиться ретроспективно и предоставлять честные отзывы об эффективности ранее принятых и реализованных решений. Эффективность новых правил и процедур может быть хорошей темой для будущих учений.
- **Не прекращайте работу** — Экосистема обмена информацией об исходных данных и полученных результатах должна представлять собой непрерывный процесс, комплексный и динамичный, поскольку недостаточный обмен информацией или неполная оценка могут привести к появлению новых слабых мест в системе. □

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

# *Албания создает*
# НАЦИОНАЛЬНЫЕ КИБЕРКАДРЫ

## *Анализ несоответствий в системе образования, профессиональной подготовки и сертификации в сфере кибербезопасности*

**Д-р Вилма Томцо**, генеральный директор, и **Клорента Януши**, эксперт по информационной безопасности,
Национальное агентство по электронной сертификации и кибербезопасности, Совет министров Республики Албания

Кибербезопасность находится в числе национальных приоритетов. При таком беспрецедентно быстром распространении коммуникационных технологий кибербезопасность, функциональная совместимость и цифровая трансформация стали основными темами обсуждения в современной цифровой среде. Принимая во внимание такое явление как «утечка мозгов», мы уже находимся в кризисной ситуации, когда мы не производим необходимое интернет-индустрии количество квалифицированных кадров. Финансовые инвестиции, возможно, уже не являются основным препятствием, как это было раньше, а вот организациям необходимо иметь четкое представление о своих ресурсах, активах и уровне компетентности сотрудников, чтобы они смогли увидеть свои слабые места.

Общий подход сегодня к проблеме нехватки кадров состоит в кратковременном латании дыр. Университеты ввели в свои учебные программы степени бакалавра и магистра по специальности кибербезопасности, однако составители этих программ должны учитывать стоящие перед ними проблемы по мере того, как цифровая среда эволюционирует колоссальными темпами. Динамизм этой сферы деятельности должен привести к четкому пониманию того факта, что реалии фундаментально отличаются от существующих учебных планов. Такое понимание очень важно в наших усилиях по сокращению нехватки специалистов, которые включают привлечение большего числа женщин и достижения более высокого уровня диверсификации в компьютерной сфере.

### Законодательный рамки

Европейский союз регулирует область кибербезопасности посредством общих законодательных рамок, частью которых является принятая Директива относительно безопасности сетей и информационных систем (Директива NIS). Албания, выполняя свои обязательства кандидата в члены ЕС, частично приняла Директиву NIS, одобрив Закон № 2/2017 «О кибербезопасности». Закон наделяет Национальное агентство по электронной сертификации и кибербезопасности (NAECCS) полномочиями надзора и реализации, и при этом NAECCS, в соответствии с законом, выполняет функции национальной Группы реагирования на инциденты в сфере кибербезопасности (CSIRT). Для выполнения этих функциональных задач NAECCS приняло методологию для организации и функционирования CSIRT на национальном уровне. В методологии закреплено обязательство создать CSIRT на каждом объекте критической и важной информационной инфраструктуры (CIIIO). Список операторов таких объектов утвержден Советом министров и обновляется каждые два года.

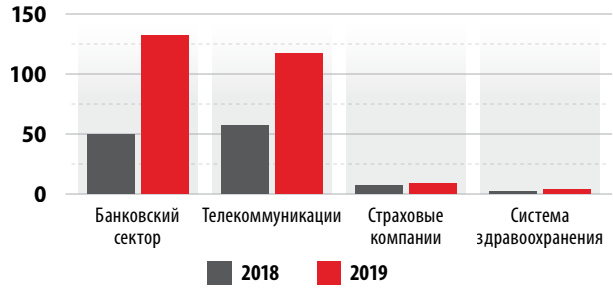
Закон «О кибербезопасности» и соответствующие подзаконные акты определяют обязательства для всех CIIIO следующим образом:

- В структуре CSIRT каждого сектора создать специальные должности для экспертов по кибербезопасности.
- Повысить функциональность системы путем

принятия дополнительных мер по повышению уровня безопасности и координации действий с национальным CSIRT для реагирования на кибер-инциденты в режиме реального времени.
- Повышать технические и профессиональные способности сотрудников путем организации специального обучения в сфере кибербезопасности, проведения киберучений и т.д.

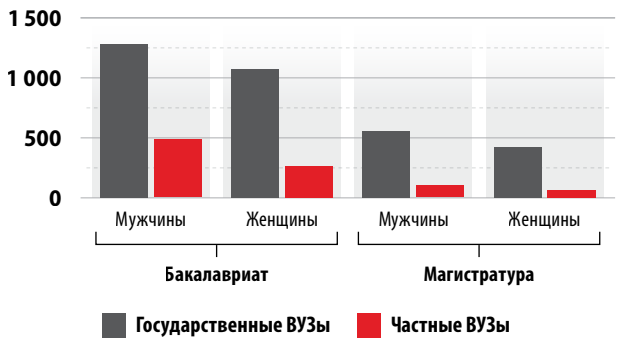
Выполнение этого закона и соответствующих подзаконных актов отражено на Рисунке 1. После создания законодательной базы в сфере кибербезопасности СПІО увеличили количество должностей, имеющих прямое отношение к кибербезопасности. На Рисунке 1 изображен один из наиболее динамичных секторов, основанных на Директиве NIS. NAECCS периодически проводит киберучения и теоретические упражнения в целях повышения квалификации экспертов с тем, чтобы создать в Албании более безопасную кибернетическую экосистему. За этот же самый период СПІО подтвердили свою решимость в реализации проектов в сфере кибербезопасности, инвестировав в них 1,1 млн. евро.

Рисунок 1: **Количество экспертов по кибербезопасности на объектах критически важной инфраструктуры**




Источники: д-р Вилма Томцо и Клорента Януши

Рисунок 2: **Студенты, изучающие предмет кибербезопасности в ВУЗах Албании, 2019 г.**




Источники: д-р Вилма Томцо и Клорента Януши

Мощные потоки воды проходят через дамбу в г. Вау-и-Даес на реке Дрин в северной части Албании. Наличие квалифицированных кадров в сфере кибербезопасности крайне необходимо для защиты объектов критически важной инфраструктуры, таких как эта дамба. РЕЙТЕР

Все государственные учреждения сталкиваются с общей угрозой, которая может постепенно разрушить их механизмы защиты: с «утечкой мозгов» в секторе кибербезопасности. В числе факторов, вызывающих это явление – низкие зарплаты в госучреждениях и большой процент скучной ручной работы при обслуживании существующих систем, что часто приводит к неудовлетворенности высококлассных специалистов и их уходу. Исследование показало, что только 35% сотрудников, отвечающих за кибербезопасность в опрошенных правительственных ведомствах, имеют действительный международный сертификат и являются «сертифицированным главным экспертом по информационной безопасности» (CCISO), «сертифицированным профессионалом в области информационной безопасности», или обладателем сертификата ISO 27001 (Международная организация по стандартизации).

## Студенты, изучающие предмет кибербезопасности

Проведенный NAECCS в 2019 г. опрос в высших учебных заведениях Албании проанализировал такую информацию о студентах как их демографические особенности, гендерная принадлежность и уровень обучения (бакалавриат и магистратура). Рисунок 2 показывает разницу в количестве студентов мужского и женского пола, дает представление о том, как после окончания учебы они увеличат уровень кибер-экпетизы на рынке труда.

Лекции по вопросам, относящимся к кибербезопасности, введены в учебные программы 20% государственных университетов, в 15% частных университетов и в 10% центров профессионального обучения. NAECCS играет ключевую роль в увеличение числа экспертов в сфере кибербезопасности в Албании путем увеличения числа студентов, проходящих обучение по этому предмету. В 2017 г. NAECCS организовало Албанскую киберакадемию (ACA) с целью повышения интереса студентов к области кибербезопасности. ACA приглашает албанских и зарубежных экспертов в сфере кибербезопасности и студентов, изучающих информационные и коммуникационные технологии (ИКТ), углубить свои знания и расширить сеть профессиональных контактов.

Ежегодно NAECCS организует конференции на тему «Женщины в сфере информационных и коммуникационных технологий», в ходе которых женщины, работающие в области ИКТ, делятся своими идеями и заинтересовывают молодых людей в выборе карьеры в секторе кибербезопасности. Женщины в Албании занимают самые высокие руководящие посты в области ИКТ, работая на должностях генеральных директоров, директоров по ИКТ и директоров по информационной безопасности.

## Заключение

У организаций есть четко определенная обязанность повышать качество обучения своего персонала, работающего в сфере безопасности информационных технологий, разрабатывать стимуляционные пакеты для удержания сотрудников и, что особенно важно, привлекать молодых специалистов. В будущем мы планируем введение предмета кибербезопасности во все учебные программы, поскольку все студенты ВУЗов являются потенциальными кандидатами на должности, имеющие отношение к области кибербезопасности. Профессиональное развитие кадров чрезвычайно важно, поскольку сама природа киберугроз эволюционирует чрезвычайно быстро. У специалистов имеется много способов повышения своих профессиональных навыков, включая получение сертификатов и дополнительных университетских степеней, а также прохождение практических курсов для развития особых технических навыков.

Две шестнадцатилетние девушки, Деа Рожани и Йонада Шукараси, создали компьютерное приложение, помогающее бороться с домашним насилием. Все больше женщин стремятся сделать карьеру в сфере информационных технологий, что поможет сократить нехватку специалистов в этой области. РЕЙТЕР

Поскольку утверждение университетских учебных программ занимает довольно много времени, то определенную помощь могут оказывать центры профессионального обучения, организуя краткосрочные курсы для техников, аналитиков и аудиторов, работающих в сфере информационной безопасности.

Статистика показывает, что албанские женщины более сосредоточены на своей работе и более преданы ей, чем мужчины, и поэтому крайне необходимо делать все, чтобы привлекать больше женщин на работу в сектор кибербезопасности. Этого можно достичь путем проведения информационных кампаний и различных мероприятий, таких как конкурсы, хакатоны, конференции, университетские распределения выпускников и др. □

# РАЗРЫВАЯ «ТРЕУГОЛЬНИК» НЕДОВЕРИЯ

**Д-р Максимилиан Шуберт,** генеральный секретарь австрийской Ассоциации Интернет-провайдеров

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

# Для решения проблем кибербезопасности необходимы взаимное уважение и доверие

Более 20 лет большая часть деятельности в режиме онлайн рассматривалась как позитивное и расширяющее человеческие возможности явление, вносящее в жизнь общества много полезных изменений. К сожалению, сегодня некоторые люди используют эти технологии во зло. У Интернет-провайдеров, правоохранительных органов и гражданского общества одна общая цель – сделать Интернет более безопасным. Однако, они подходят к решению проблем с разных позиций: правоохранительные органы хотят поймать преступников, Интернет-провайдеры стремятся удовлетворить нужды своих клиентов, а гражданское общество хочет защитить основные права человека.

Эта статья основывается на опыте автора, который был участником Программы по изучению вопросов кибербезопасности (ПВКБ) в Европейском центре исследований безопасности им. Джорджа Маршалла в 2017 г. Цель статьи – показать необходимость доверительного сотрудничества всех заинтересованных сторон и попытаться выявить существующие ныне предубеждения.

При участии в таких программах как ПВКБ, отдельным представителям Интернет-индустрии очень трудно выражать мнения от имени всего этого сегмента, поскольку по большинству вопросов нет единых взглядов. Большинство людей ошибочно могут предполагать, что работающие в Интернет-индустрии специалисты в основной своей массе принадлежат к одной и той же культуре. На самом же деле во многом их взгляды определяются культурными и историческими факторами. Например, в то время как жители стран с давно установившейся демократией (например, Великобритании) проявляют относительно высокий уровень доверия к государственным институтам и готовы принять большую степень общественного наблюдения за своей деятельностью, в странах, где в прошлом наблюдалось или в настоящее время наблюдается недоверие к властям (например, в Чили), люди гораздо более чувствительно относятся к вопросам конфиденциальности и государственного надзора.

В контексте программы ПВКБ Интернет-индустрия неоднократно подвергалась критике за недостаточный уровень сотрудничества, ее упрекали в том, что она еще больше усугубляет проблемы вместо того, чтобы способствовать их решению. В процессе дискуссий становилось очевидным, что многие из политических, социальных и экономических проблем просто проецировались на Интернет-индустрию. Зачастую выдвигались огульные обвинения в том, что Интернет-индустрия не желает «делать свою часть работы». В этих условиях казалось совершенно неизбежным, что управление этой сферой будет передано правительству либо путем принятия дополнительных регулятивных положений, либо прямой передачей основных функций государственным органам.

Недостаток доверия также рассматривался как фактор, который мешает государственному сектору в его «битве за таланты». Государственные субъекты часто чувствуют себя в невыгодном положении по сравнению с частным сектором; как работодатели они менее привлекательны, в частности, из-за жестких условий приема на работу, уровня зарплат и правил конфиденциальности. Тем не менее, работодатели из государственного сектора могут быть очень изобретательными в своем стремлении заполучить желаемые кадры: одни ведут эмоциональные переговоры с кандидатами, другие предлагают своим сотрудникам привлекательные рабочие обязанности, а также обширные возможности обучения и достаточное количество времени, чтобы освоить все детали постоянно возникающих технических проблем в этой стремительно развивающейся сфере индустрии.

## Идеологические различия в смоделированном сценарии

Противоречие между такими аспектами как конфиденциальность, с одной стороны, и безопасность, с другой, часто становилась предметом обсуждения, но, к сожалению, решить эту проблему никто не пытался. Различие взглядов по этому вопросу лучше всего проявилось в контексте онлайновой смоделированной игры под названием CounterNet. Суть этой игры для одного игрока в том, чтобы показать, как террористы используют Интернет и социальные сети в своих различных преступных целях. Игрок принимает на себя роль представителя государственного учреждения, который обязан отследить и в конечном итоге предотвратить нападение вымышленной террористической группировки, стремящейся нанести экологический ущерб. В определенный момент игра выходит на новый уровень при условии, что дается указание отслеживать телекоммуникации подозреваемых в преступной деятельности без учета существующего законодательства, таким образом сознательно игнорируя и преднамеренно нарушая основные права человека. Если же игрок принимает решение не давать такое указание, то тогда он лишается части уже заработанных баллов и не выходит на новый уровень игры.

В ходе последующего обсуждения игры это требование нарушить закон вызвало ожесточенные дебаты. В то время как значительное число участников отказались дальше действовать без законодательной основы, другие

Специалист-аналитик просматривает данные социальных сетей в Общенациональном информационно-аналитическом центре в г. Солт Лейк Сити, штат Юта, США. GETTY IMAGES

сочли оправданным игнорирование основных прав человека в условиях, когда, по сценарию игры, террористическое нападение было неизбежным. Этот смоделированный сценарий отлично продемонстрировал различия в идеологиях и подходах различных заинтересованных сторон и предоставил достаточно времени для детального обсуждения.

## Треугольник недоверия

Не будет преувеличением сказать, что нынешние отношения между Интернет-индустрией, гражданским обществом и государственными органами в сфере кибербезопасности приводят к конфликтам и неправильным представлениям. При этом в стремлении достичь общую цель – создать «безопасное» киберпространство – все эти субъекты зависят друг от друга. И если раньше государственным органам было вполне достаточно просто исходить в этом вопросе из своих конституционных полномочий, то в эпоху «фейковых новостей» и целенаправленных национальных кампаний дезинформации государственным субъектам, таким как армия или правоохранительные органы, становится все труднее оправдывать свои действия. Эти сомнения должны носить транспарентный характер и открыто обсуждаться.

Пока три заинтересованные стороны – гражданское общество, Интернет-индустрия и государственный сектор (правоохранительные органы и военные) – будут и дальше огульно и непримиримо обвинять друг друга, взаимного уважения добиться не удастся. Такие обвинения мешают созданию обстановки доверия, формирующей основу необходимого сотрудничества между всеми субъектами при решении проблем, возникающих в киберсреде. Если разбить этот «треугольник недоверия» на отдельные элементы, то наиболее распространенные предубеждения можно суммировать следующим образом:

***Гражданское общество*** не доверяет Интернет-индустрии из-за отсутствия прозрачности в таких вопросах как мотивация и степень сотрудничества с правоохранительными органами. Из-за необходимости режима секретности и, следовательно, недостаточности количества информации, доступной гражданскому обществу, правоохранительные органы и армия часто представляются как институты, сознательно преувеличивающие опасности с тем, чтобы расширить свое влияние и контроль, тем самым ставя под угрозу гражданские свободы и, в конечном итоге, всю демократическую систему.

***Правоохранительные органы и армия*** обвиняют гражданское общество в наивности и в отказе принять реалии проблем в киберсфере. Интернет-индустрия подвергается критике за нежелание нести ответственность за те угрозы, которые она создает, и за использование вопроса об основных правах человека в качестве предлога при отказе от сотрудничества с правоохранительными органами.

***Интернет-индустрия*** критикует гражданское общество за чрезмерно резкое реагирование на аспект конфиденциальности, что мешает внедрению инноваций. В то же время считается, что правоохранительные органы и армия чересчур узко смотрят на эту сферу, игнорируя отрицательные последствия своих действий

## «Треугольник недоверия»


для развития бизнеса и дальнейшего продвижения Интернета и других кибертехнологий.

Именно в силу этих причин инициативы наподобие программы ПВКБ представляют собой отличную возможность выявить существующие предубеждения и со временем преодолеть их. Чтобы поддержать этот процесс, стоит подумать о дальнейшем расширении числа участников этой программы; в их число должны быть включены не только представители Интернет-индустрии, но также и члены гражданского общества. Это поможет ослабить предубеждения между этими субъектами, а также добиться лучшего понимания предвзятого отношения, существующего в армии и в правоохранительных органах.

***Доверие – это необходимое условие для успешного сотрудничества между Интернет-индустрией и правоохранительными органами.***

Хотя уровень сотрудничества между Интернет-индустрией и правоохранительными органами часто считается недостаточным, стремление понять корень проблемы уже привело к значительному прогрессу. Что удивительно, помимо проблем юридического и регулятивного характера, зачастую обе стороны сталкиваются с проблемами, связанными с практическими действиями. Это видно из последнего отчета Европола «SIRIUS» по вопросу взаимного предоставления странами электронных улик совершения преступлений, в котором обозначены наиболее распространенные практические проблемы.

В числе наиболее часто встречающихся проблем, с которыми сталкиваются правоохранительные органы – незнание, к кому обратиться за информацией, несоблюдение формальных требований (например, отсутствие необходимых подписей), отказ в предоставлении запрашиваемой информации (в том числе и из-за отсутствия законодательной базы, регулирующей этот вопрос) и отсутствие единой позиции относительно того, как пересылать запросы (например, правоохранительные органы настаивают на том, чтобы им сообщения присылали по факсу, а не электронной почтой). С целью разрешить эти вопросы ряд европейских стран, например, Голландия, создали единый национальный контактный орган со специально обученным и оснащенным штатом сотрудников для обмена информацией с Интернет-индустрией, что привело к существенному увеличению числа успешно отправленных заявок. Еще одним ключом к успеху в этих странах была способность создать доверительные отношения с Интернет-индустрией. Такие отношения можно инициировать разными способами – от совместного участия с представителями индустрии в одних и тех же мероприятиях до приглашения их на неформальную встречу за завтраком, чтобы обсудить практические вопросы.

Таким образом, совместное решение практических проблем привело к новому уровню сотрудничества, при котором почти во всех случаях, когда Интернет-провайдеры отказываются передать правоохранительным органам запрашиваемую информацию, они это делают не потому что не хотят помочь правоохранительным органам, а потому что они не в состоянии помочь по техническим причинам или в силу юридических требований.

Для того, чтобы преодолеть эти различия, стремясь к созданию более безопасного киберпространства, необходимо проводить серьезные дискуссии. Независимо от того, насколько разочаровывающим и затратным может показаться это диалог, без него не обойтись. Программа ПВКБ и Центр им. Маршалла могли бы сыграть ключевую роль в создании атмосферы доверия между различными заинтересованными сторонами, стремящимися достичь общую цель – более безопасный Интернет для каждого пользователя. Даже если мнения по некоторым вопросам и будут расходиться в будущем, доверительные отношения между Интернет-провайдерами, правоохранительными органами и гражданским обществом все равно будут способствовать обмену знаниями ради достижения этой общей цели. □

# ОБЕСПЕЧИВАЯ БЕЗОПАСНОЕ БУДУЩЕЕ

## *Безопасность детей в сети – план действий*

**Рэки Сей**

Начальник Управления безопасности информационных систем и цифрового доверия,
Министерство цифровой экономики и телекоммуникаций Сенегала

Дети и молодые люди находятся в числе наиболее активных пользователей мобильных технологий. И хотя этот факт может иметь позитивное влияние на их образование и жизнь, мобильные технологии также могут наносить вред. Безопасность детей в киберпространстве необходима так же, как и их защита в реальном физическом мире. Родители, правительства и частные компании могут играть важную роль в защите и поддержке пользующихся Интернетом детей и помочь им избежать девиантного поведения с его губительными последствиями. Чтобы справиться с этой проблемой, для Сенегала было чрезвычайно важно подготовить кадры для информационной безопасности детей в сети на национальном уровне и провести в жизнь план действий.

## ПЛАН БЕЗОПАСНОСТИ ДЕТЕЙ В СЕТИ (ПБДС)


Согласно оценкам, в Сенегале Интернетом пользуется 68% населения. Учитывая, что из 10,4 млн. интернет-абонентов в стране 41% составляют дети до 15 лет, правительство сделало ПБДС своим приоритетом, рассчитывая на сближение и взаимодействие инициатив в этой области, силу институтов, а также влияние семьи и общественных организаций.

В этом контексте, руководствуясь стратегией «Цифровой Сенегал до 2025 г.», правительство Сенегала одобрило Стратегию национальной кибербезопасности. В этом документе ставится цель создания в стране к 2022 г. «киберпространства доверия, безопасности и жизнестойкости для всех» и единой культуры кибербезопасности. Документ подчеркивает особую задачу: «Повышение информированности всех заинтересованных групп и широкой общественности о рисках безопасности в киберпространстве».

Национальный план действий ПБДС направлен на выполнение этой стратегической задачи. Этот план, демонстрирующий решимость Сенегала защитить детей от опасностей Интернета, базируется на шести основных элементах:

1. Государственная политика и управление
2. Законность
3. Общество
4. Средства массовой информации и коммуникации
5. Жертвы
6. Интернет-провайдеры и промышленность

## ШЕСТЬ ОСНОВНЫХ ЭЛЕМЕНТОВ

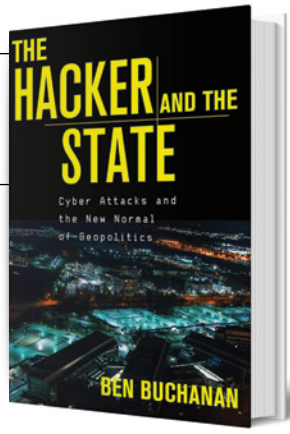
Каждый элемент подразумевает определенную деятельность, например, повышение информированности и обучение детей, родителей и всех заинтересованных сторон, а также разработку технических систем заботы о жертвах губительного влияния Интернета с тем, чтобы обеспечить в современном цифровом мире баланс между безопасностью детей и предоставлением им более широкого спектра возможностей использования мобильных платформ и информационных и коммуникационных технологий (ИКТ).

Реализуя это план, в частности, его первый элемент, относящийся к государственной политике и управлению, министерским указом был создан координационный комитет из ключевых фигур ПБДС, общественного и частного сектора, а также гражданского общества. Возглавляет комитет управление ИКТ Министерства цифровой экономики и коммуникаций. Оно руководит процессом реализации плана действий путем организации регулярных встреч и семинаров.

В начале каждого года комитет на основе плана действий составляет график работы на год с указанием конкретных мероприятий. Этот комитет также является органом международных контактов по всем делам, касающимся безопасности детей в сети.

Сегодняшние дети и молодые люди – это следующее поколение лидеров века кибернетики, и национальные программы уже сейчас должны отвечать их уникальным потребностям, учитывая комплексные угрозы для общества в будущем. Всеправительственный подход доказал свою эффективность. Для того, чтобы создать следующее поколение специалистов в сфере кибернетики, такие планы действий должны занять приоритетное место в обсуждении вопросов политики в сфере кибербезопасности. □

# НОВАЯ «НОРМА»




**АВТОР:** Бен Бьюкенен
**ИЗДАТЕЛЬСТВО:** Harvard University Press
**РЕЦЕНЗЕНТ:** Патрик Сван, обозреватель журнала *per Concordiam*

Кибервойна не должна была быть такой как сейчас. Мы ожидали цифровой аналог Перл Харбор, означающий первые выстрелы в большом глобальном конфликте. Как и в случае ядерной войны, это должно было бы стать киберверсией взаимного гарантированного уничтожения. Вместо этого оказалось, что эта война более эффективна, когда применяются скрытность и отрицание собственных действий в ходе постоянных раздражающих стычек в киберпространстве. Как форма государственной деятельности, они больше напоминают шпионские страсти «плаща и кинжала», чем использование огромных баллистических снарядов. Ситуация довольно парадоксальна. В то время как цифровые технологии делают все более точной доставку обычных боеприпасов к цели, кибертехнологии зачастую остаются просто грубым и бесконтрольным инструментом силы, накрывающим сразу большие площади.

Для лучшего понимания этого изменчивого феномена новой войны Бен Бьюкенен в своей книге «Хакер и государство: кибератаки и новая «норма» геополитики» дает совет. Он пишет: к действиям государства всегда надо применять два подхода: значение поданного сигнала и формирование поведения. Если вам удастся расшифровать, является ли конкретная проведенная кибероперация сигналом, демонстрирующим возможности, или формированием поведения, то вы придете к правильному пониманию того, «что все это значит».

В одном случае может посылаться сигнал противнику, чтобы он изменил свое поведение, если не хочет столкнуться с неприятными последствиями; в другом случае кибероперация определяет дальнейшее развитие событий путем создания противнику помех для продолжения его модели поведения. Бьюкенен утверждает, что киберпространство все более представляет собой универсальный инструмент для формирования геополитики и получения выгод, но при этом плохо подходит для подачи сигналов относительно собственных позиций и намерений. Он пишет, что кибервозможности должны храниться в секрете, что зачастую приводит к получению определенных выгод. Посылая сигнал, противник демонстрирует свои кибервозможности.

Бьюкенен прямо заявляет: лучшим способом разработать строгую концепцию проведения кибероперациий будет не использование знакомой парадигмы, в центре которой стоят посылаемые сигналы, а схема формирования поведения, уходящая корнями в такие концепции как шпионаж, подрывная деятельность и дестабилизация. Он добавляет: «Наибольшие выгоды из хакерской деятельности получают именно те государства, которые настойчиво перестраивают геополитическую среду под свои интересы, а не те, которые пытаются давать указания, принуждать или угрожать».

Государства прибегают к угрожающей риторике в отношении друг друга постоянно. Старые угрозы типа «мы с моей армией еще покажем тебе» уже звучат банально. Ты говоришь, что можешь вывести из строя мою энергосистему? Давай, попробуй! Но до тех пор, пока слова не будут подкреплены действиями, угроза будет восприниматься как пустое бахвальство. Даже если страна А предпримет действия против страны Б, эффект будет краткосрочный. Энергосеть будет выведена из строя и население будет испытывать неудобства и страдания. Страна Б восстановит энергосеть и усилит ее защиту. Однако, при этом страна А утратит возможности формировать поведение страны Б.

В отдельных случаях в процессе формирования поведения противника бывает необходимо, как бы непреднамеренно, послать сигнал и о своих кибервозможностях. Прицельным ударом с воздуха США убили в багдадском аэропорту командующего иранским Корпусом стражей исламской революции. Этим авиаударом американцы придали новую форму продолжающемуся конфликту с Ираном, придя к выводу, что устранение иранского командира принесет больше выгод, чем простые сигналы о том, что у них есть возможности это сделать. Несомненно, этот авиаудар заставил иранцев изменить свою модель поведения, но эти перемены не могли вернуть чрезвычайно эффективного и харизматичного военного руководителя.

Чтобы помочь читателям понять нюансы направления сигналов о возможностях и формирования поведения, Бьюкенен разбил свою книгу на главы, посвященные явлениям шпионажа, нападений и дестабилизации. Он вспоминает послание стратега международных отношений Томаса Шеллинга, который во главу угла теории о войне поставил процесс переговоров. Посылая противнику сигнал о своей «возможности нанести ему ущерб», вы принуждаете противника хотя бы частично уступить вашей воле в стремлении избежать губительных последствий. Посылаемые сигналы недвусмысленны и убедительны. Но опять, применительно к кибероперациям проблема в том, что эти сигналы довольно редко бывают четкими, поскольку по своей природе они должны иметь неясное происхождение. Таким образом, вместо того, чтобы посылать Ирану сигналы, что США имеют кибервозможности нарушить работу его ядерного реактора, если он сохранит свое стремление к созданию атомной бомбы, США, предположительно, просто тихо провели

диверсию против иранского ядерного объекта с использованием компьютерного сетевого вируса Stuxnet. Эта операция по формированию поведения противника подорвала уверенность Ирана в его возможности управлять центрифугой ядерного реактора, поскольку он не знал наверняка, была ли это кибератака противника или же некомпетентность собственных инженеров.

В свою очередь, когда Иран предпринял кибератаку на нефтяную компанию «Aramco» в Саудовской Аравии с целью сигнализировать о своем недовольстве внешней политикой саудовцев, эта атака не привела к переменам в поведении Саудовской Аравии. Одной из причин такого результата было то, что эта атака была проведена скрытно хакерами третьей стороны с тем, чтобы Иран мог заявить, что его государственные структуры не имеют к этому никакого отношения. Бьюкенен утверждает, что сигналы с угрозами более эффективны, если у государства имеется готовность выполнить эти угрозы. За угрозами Ирана не последовали действия, что в конечном итоге свело на нет те «победы», которые одержали его хакеры. Еще одним аспектом эффективных и тонких геополитических сигналов, на который ссылается Бьюкенен, является возможность применения тщательно отмеренного объема насильственных мер с угрозой их дальнейшей эскалации. После кибернападения на «Aramco» саудовцы не опасались последующего нападения и не изменили своего поведения в угоду Ирану.

Приводимые Бьюкененом примеры демонстрируют всю головоломную ситуацию, связанную с кибероперациями на геополитическом уровне. Государства используют хакеров, которые действуют от их имени. Государство отрицает любую причастность, чтобы избежать физической войны с противником. Однако, сигнал может не достичь цели, если окажется невозможным отследить с большой степенью уверенности, какое же именно государство стоит за кибернападением. Кроме того, если спонсирующее нападение государство не руководит этим нападением напрямую, то посланный сигнал может оказаться нечетким и двусмысленным.

Бьюкенен указывает на три замеченные им характеристики хакерской деятельности: ее универсальность как инструмента формирования геополитики, ее слабость как геополитического средства подачи сигналов и ее амбициозность, которая принимает все более агрессивный характер по мере того как современные кибероперации наращивают свои возможности. «Хакерская деятельность добилась своего признания в сценариях поведения государств». В то же время, хакерской деятельности не достает точности при нападении, поскольку кибервторжение не представляет собой предсказуемую силу, которую легко рассчитать; иными словами, при хакерских атаках невозможно нанести противнику тщательно выверенный масштаб ущерба. Это происходит потому, что при кибератаках трудно соблюдать точность в отношении их целей. Если ущерб от нападения меньше, чем запланировано, то нападающий зачастую уже не может провести атаку повторно потому, что возможности уже израсходованы или потому, что эти возможности обнаружены и против них приняты меры. А именно это и является ключом к успеху: операция должна принести ожидаемый результат и иметь возможность со временем быть повторенной. В противном случае это все равно что наобум запускать ракеты «Скад» в надежде, что они нанесут какой-то ущерб противнику. Чтобы сигнал имел запланированный эффект, нужно не просто заложить в него угрозу, но и иметь твердое намерение при необходимости эту угрозу выполнить. «В кибероперациях, в которых не подвергаются риску человеческие жизни, неясен путь эскалации, зачастую отсутствует четкий индикатор последнего шанса избежать конфликта, и в кибероперациях, которые часто утрачивают свою эффективность, когда подготовка к ним становится достоянием гласности, трудно показать четко выраженное намерение выполнить угрозу», - пишет Бьюкенен.

В старом мультипликационном сериале «Веселые мелодии» есть персонаж, который объявляет своему обидчику «Теперь между нами война». В отличие от этого в киберпространстве, как утверждает Бьюкенен, политики рассматривают кибероперации не как акты войны или даже не как общественную кризисную ситуацию, а как часть ежедневных потасовок в цифровом поле. Государства используют их в соперничестве за геополитические преимущества, и эти операции, как правило, не сдерживаются юридическими нормами, договорами или страхом перед возмездием. Это может послужить определенным объяснением, почему кибернападения не рассматриваются как акты войны – ведь в таком случае конкретное государство постоянно находилось бы в состоянии войны с целым рядом других государств, но при этом у него не было бы уверенности в том, что его контратаки направлены действительно против государства, стоявшего за первоначальным кибернападением. Без такой уверенности продолжение потасовок в цифровом пространстве представляется более привлекательной перспективой.

С одной стороны, кибероперации прямо соответствуют ситуации, некогда названной «невоенные операции», «асимметричная война» или «малая война». Они могут осуществляться в качестве отдельных независимых операций для достижения целей национальной стратегии и быть одним из вариантов возможных действий. С другой стороны, они могут проводиться параллельно с обычными наступательными военными операциями, формируя поле боя в цифровом пространстве в начале неядерных военных действий. При этом не будет иметь значения тот факт, что пришлось раскрыть свои кибервозможности, поскольку противник, подавленный обычной военной силой, просто не будет иметь времени создать защиту против подобных кибероперациий. Такой подход срабатывает в ситуации, где временной фактор играет большую роль.

Главный вывод из книги Бьюкенена заключается в необходимости точно определить, какой подход в кибервойне является более эффективным – формирование поведения противника или угрожающие сигналы. После этого государство может создать максимум кибервозможностей и при необходимости использовать их соответствующим образом против четко выраженных и предполагаемых угроз. На практике это означает противодействие государственным субъектам или хакерам, спонсируемым государством. Опыт показывает, что неправильный расчет относительно того, когда нужно использовать каждый из этих подходов, представляет собой профессиональную некомпетентность при проведении стратегических операций в киберпространстве. Учитывая то, что усилия США в сферах безопасности, коллективной обороны и региональной стабильности направлены на создание условий для минимизации конфликта и расширения возможностей для мира и процветания, то необходимо стремиться к ситуации, при которой кибероперации утратят свою необходимость и, подобно ядерному оружию, будут применяться крайне редко или не применяться вообще. □

# 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

https://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 инициировать процесс. Запрос можно направить по электронному адресу: registrar@marshallcenter.org

**Обновленное расписание курсов выставлено на вебсайте Центра им.Маршалла**

## ПРОГРАММА ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ (ПАСС)

Основной курс очного обучения Центра им. Маршалла 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.

## ПРОГРАММА «БОРЬБА С ТРАНСНАЦИОНАЛЬНОЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ» (БТОП)

В центре внимания этой программы очного обучения находятся угрозы национальной безопасности, исходящие от контрабандных операций и других преступлений. Курс рассчитан на правительственных и государственных чиновников и практических работников, которые занимаются разработкой политики, правоохранительной и разведывательной деятельностью, а также операциями перехвата.

## ПРОГРАММА «ТЕРРОРИЗМ И ВОПРОСЫ БЕЗОПАСНОСТИ» (ПТВБ)

Эта 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.

## СЕМИНАР ДЛЯ ВЫСШЕГО РУКОВОДЯЩЕГО СОСТАВА (СВРС)

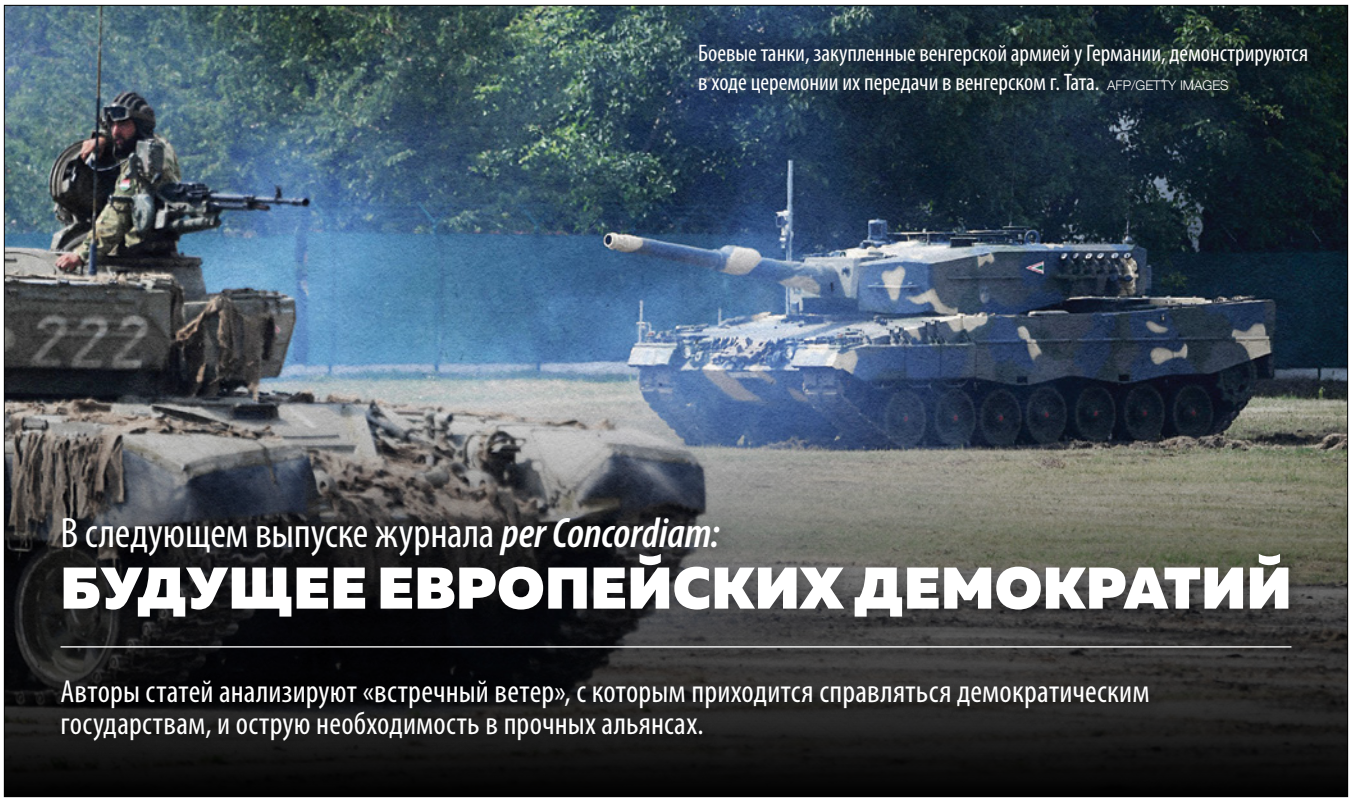
Это интенсивная программа, посвященная новым ключевым глобальным тенденциям, которые могут привести к появлению новых точек зрения, концепций и совместных обсуждений, а также возможных решений. Программа предназначена для высшего офицерского состава, дипломатов высокого ранга, послов, министров, заместителей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

## 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.

## СЕМИНАР ПО РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ (СРБ)

Цель семинара – систематический анализ характера отдельных кризисов, влияния региональных субъектов, а также воздействия международных мер помощи.



Боевые танки, закупленные венгерской армией у Германии, демонстрируются в ходе церемонии их передачи в венгерском г. Тата. AFP/GETTY IMAGES

В следующем выпуске журнала *per Concordiam:*

## БУДУЩЕЕ ЕВРОПЕЙСКИХ ДЕМОКРАТИЙ

Авторы статей анализируют «встречный ветер», с которым приходится справляться демократическим государствам, и острую необходимость в прочных альянсах.

# ПРОГРАММЫ ДЛЯ ВЫПУСКНИКОВ


**Кристофер Бурелли**
Директор, программ для выпускников
тел +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org
Языки: английский, словацкий, итальянский, немецкий


## Специалисты по связям с выпускниками


**Дру Бек**
Западные Балканы, франкоговорящая Африка
Языки: английский, французский
тел + 49-(0)8821-750-2291
ryan.beck@marshallcenter.org

**Йохен Рихтер**
Западная Европа
Языки: немецкий, английский
тел + 49-(0)8821-750-2814
jochen.richter@marshallcenter.org

**Марк Джонсон**
Восточная Европа, Кавказ, Центральная Азия; Специалист по кибервопросам
Языки: английский, русский, французский
тел + 49-(0)8821-750-2014
marc.johnson@marshallcenter.org

**Фрэнк Льюис**
«Вышеградская четверка», Прибалтика, Ближний Восток, Южная и Восточная Азия; специалист по противодействию терроризму
Языки: английский, немецкий
тел + 49-(0)8821-750-2112
frank.lewis@marshallcenter.org

**Донна Джанка**
Северная и Южная Америка, англоговорящая Африка, Восточные Балканы, Монголия; специалист по борьбе с транснациональной организованной преступностью (БТОП)
Языки: английский, немецкий
тел + 49-(0)8821-750-2689
nadonya.janca@marshallcenter.org



**mcalumni@marshallcenter.org**

## Подать материал для публикации

Отправляйте статьи и отзывы в Центр им. Маршалла по адресу: **editor@perconcordiam.org**

## 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* в интернете по адресу:
Центр им. Маршалла: **https://www.marshallcenter.org**
Фейсбук: **https://www.facebook.com/PerConcordiam**
Твиттер: **https://www.twitter.com/per_concordiam**
GlobalNET портал: **https://members.marshallcenter.org**
Цифровая версия: **https://perconcordiam.com**


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

ФОТОГРАФИЯ ПРЕДОСТАВЛЕНА ЦЕНТРОМ ИМ. МАРШАЛЛА