TOM 9, № 1, 2018

per Concordiam

Журнал по проблемам безопасности и обороны Европы

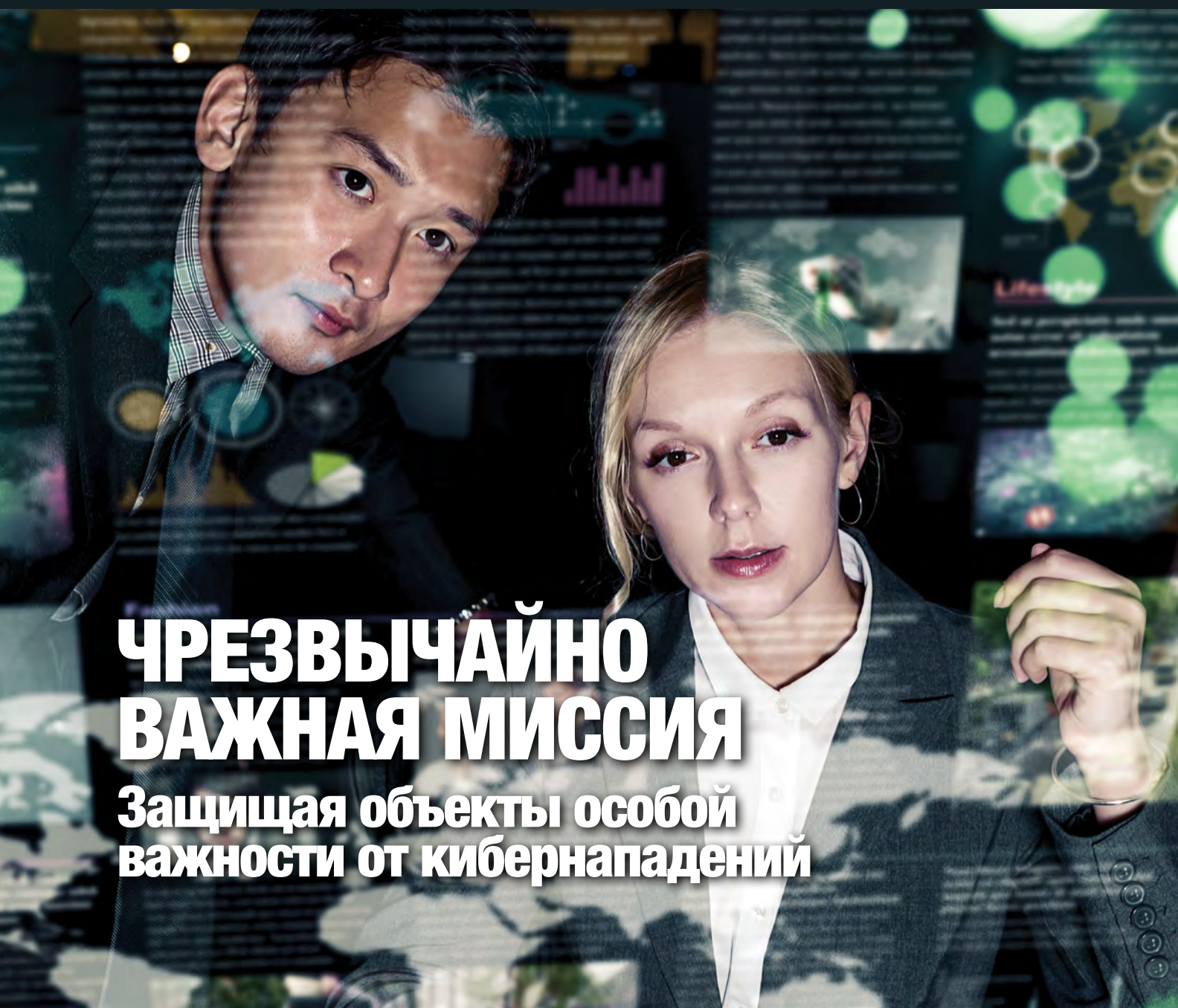
■ **КИБЕРВОЙНА В УКРАИНЕ**
За нападениями стоит российская доктрина

■ **СОЗДАВАЯ ЦИФРОВУЮ ОБОРОНУ**
Крайне необходимо партнерство государственного и частного секторов

■ **СИЛА ЖИЗНЕСТОЙКОСТИ**
Круглосуточное противостояние нападениям

■ **ИСПОЛЬЗУЯ СТРАТЕГИЧЕСКОЕ ПРЕДВИДЕНИЕ**
Делая киберпространство безопасным

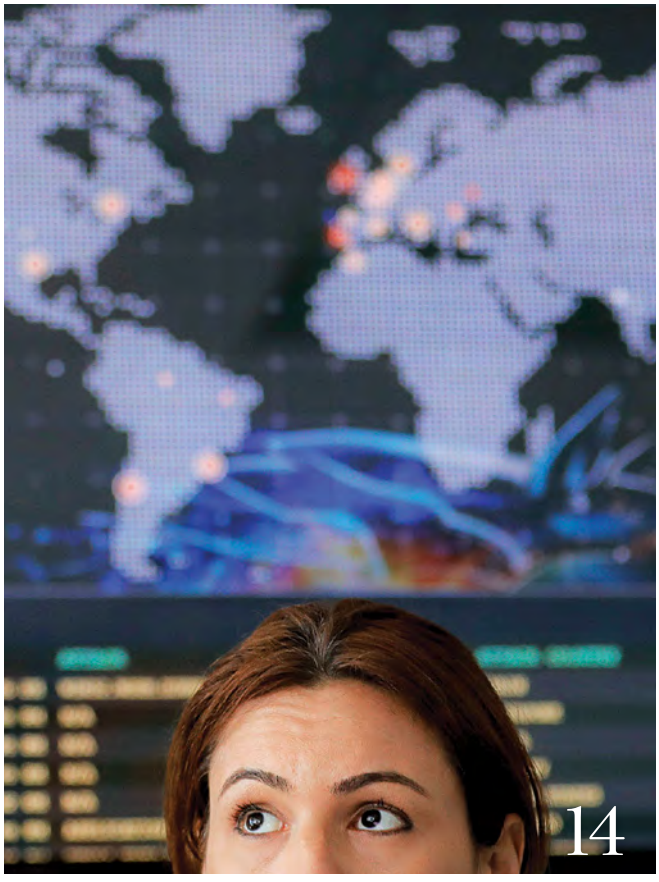
ПЛЮС
Создание сил киберрезерва в Грузии
Чешская Республика все эффективнее противостоит нападениям
Быстрое развитие интернета в Косово приводит к проблемам



ЧРЕЗВЫЧАЙНО ВАЖНАЯ МИССИЯ

Защищая объекты особой важности от кибернападений

основные статьи



разделы

В каждом номере

БЕЗОПАСНОСТЬ

ПОЛИТИКА

СОТРУДНИЧЕСТВО

на обложке:

Создание защиты от растущего числа кибератак требует планирования, взаимодействия и исполнения. ISTOCK

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Представляем вашему вниманию 33-й выпуск журнала *per Concordiam*. Этот специальный «кибернетический» выпуск освещает широкий круг тем, связанных с кибербезопасностью, однако, у всех у них единая задача: определить наиболее эффективные пути защиты объектов критически важной инфраструктуры от все более изощренных угроз со стороны отдельных государств, негосударственных образований, а также спонсируемых государствами субъектов. Последние несколько лет изощренность киберугроз для национальной безопасности растет в геометрической прогрессии. Как в региональном, так и в глобальном плане уровень этих угроз различный в зависимости от степени «пробиваемости» интернета и мобильных коммуникаций; также свою роль играет неравномерное распределение по миру знаний и опыта в конкретных областях. Таким образом, глобальная природа киберпространства делает для всех в одинаковой степени важным рассмотрение происходящих в реальном мире кибератак, а также современных тенденций в этой области.

Киберпреступления остаются одной из наиболее серьезных транснациональных угроз, и основной их мотивацией является возможность значительного финансового обогащения. В 2017 г. вирусы-вымогатели, такие как WannaCry, продемонстрировали, насколько уязвимы перед криминальными структурами современные общества, зависимые от информационных технологий. Северная Корея подозревается в создании вируса WannaCry, который зашифровывал коммерческую и личную информацию, а преступники расшифровывали только после уплаты выкупа.

Другие страны, в частности, Россия, активно составляют карты энергетических и оптоволоконных сетей потенциальных противников, как считается, для того, чтобы получить геополитические преимущества. Эксперты сходятся во мнении относительно того, что события в Украине стали своеобразным полигоном использования киберсредств в асимметричной войне. Манипулирование объектами критически важной инфраструктуры в качестве дополнительного рычага давления было очевидным в случае с Украиной, где имели место отключения электроэнергии на промышленных предприятиях в Киеве, вмешательства в финансовые системы страны, а также внедрение в компьютерные сети других вирусов, таких как NotPetya.

Кибербезопасность все меньше и меньше становится функцией только правительств и все больше превращается в область, получающую преимущества от сотрудничества между государственным и частным секторами. Многие аспекты кибербезопасности, которыми пользуются криминальные структуры, такие как уязвимые места в цепочке поставок и проблемы шифрования, имеют существенный компонент участия частного сектора.

В этот выпуск заметный вклад внесли эксперты в конкретных областях и профессионалы в сфере компьютерных сетей из многих стран мира, чьи статьи дают оценку недостаткам систем кибербезопасности на объектах критически важной инфраструктуры и предлагают новые подходы к обеспечению защиты и жизнестойкости компьютерных сетей. Читателям понравятся статьи, описывающие установление партнерства между общественным и частным секторами, обмен информацией в целях повышения эффективности управления рисками в сфере кибербезопасности и сопротивляемости сетей, а также чрезвычайно важную роль непрерывной работы над созданием киберстратегии, выработки политики и законодательной базы в целях уменьшения последствий возможных кибератак.

Программа исследований вопросов кибербезопасности (ПИКБ) в Центре им. Маршалла является первой такого рода программой, которая делает упор на разработке стратегии и планирования в рамках всеправительственного подхода и партнерства между общественным и частным секторами, а также транснационального сотрудничества. ПИКБ прививает в обществе понимание компьютерной экосистемы и масштабов современных угроз. Работая над этим, ПИКБ создает общее знание лексикона, примеров наиболее эффективных решений и современных инициатив, проходящих апробацию в общественном и частном секторах.

Мне приятно выступить с предисловием к этому выпуску *per Concordiam*, посвященному аспектам кибербезопасности, и отдать должное всем его авторам, многие из которых являются выпускниками ПИКБ. Мы приветствуем ваши комментарии и отклики на эти статьи и высказанные мнения, и собираемся продолжить этот диалог в будущих выпусках журнала, посвященных вопросам киберпространства. Пожалуйста, связывайтесь с нами по электронной почте по адресу editor@perconcordium.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.

Хафизе Байрами работает в должности начальника отдела информационных технологий (ИТ) в Министерстве сил безопасности Косово с 2009 г. и является членом Национального совета кибербезопасности с 2016 г. Хафизе имеет степень магистра в области телекоммуникаций от Университета Приштины. Она также проработала два года инженером ИТ в частном секторе. Хафизе является выпускницей Центра им. Маршалла, где занималась по «Программе исследований кибербезопасности» и также участвовала в работе «Группы по интересам – специалистов по кибербезопасности» в 2017 г.

Подполковник д-р Дарко Галинец – руководитель секции контроля и безопасности информационных систем в Секторе информационных и коммуникационных систем в Министерстве обороны Хорватии. В министерстве он занимал много должностей, связанных с информационными и коммуникационными системами. Был в числе тех, кто отвечал за соблюдение «Обязательств перед НАТО по киберзащите». Он является выпускником Центра им. Маршалла, где занимался по «Программе исследований кибербезопасности». Его исследовательская работа связана с вопросами кибербезопасности и киберзащиты.

Андрия Готсиридзе был директором Бюро кибербезопасности в Министерстве обороны Грузии с 2014 г. по 2016 г. Он был генеральным инспектором министерства, и сферой его деятельности были реформа сектора безопасности, борьба с коррупцией и деятельность иностранных разведорганов. Под его руководством Бюро кибербезопасности Министерства обороны разработало первые в Грузии стратегию и принципы киберзащиты, он также начал работать над рядом проектов в сфере кибербезопасности. В настоящее время участвует в нескольких проектах в качестве консультанта по кибербезопасности в грузинском Агентстве инноваций и технологий.

Мартин Конечны – аналитик в Национальном агентстве компьютерной и информационной безопасности Чешской Республики, где отвечает за Отдел нормативно-правового регулирования и аудитов. Он получил степень магистра от Технического Университета в Брно. Основная область его опыта и знаний – системы управления безопасностью сетей.

Полковник Виктор Лисаконов – начальник Управления информационного обеспечения при Генеральном штабе Вооруженных Сил Украины. Он участвовал в создании системы информационного обеспечения и киберзащиты в украинских вооруженных силах. На протяжении 30-летней карьеры занимал различные командные и штабные должности и имеет опыт в проведении миротворческих операций. В настоящее время его деятельность сосредоточена на развитии возможностей киберзащиты в военной сфере.

Мака Петриашвили работает в Министерстве обороны Грузии с 1999 г. и специализируется на вопросах кибербезопасности, военной разведки, оборонной политики и планирования, анализа личного состава и стратегической обороны. Она работала в качестве консультанта по вопросам кадров и организационного развития в Бюро кибербезопасности и в 2015-2016 гг. координировала проект по обеспечению информированности населения по вопросам кибербезопасности. Также участвует в программе обучения по вопросам кибербезопасности и в разработке общей справочной программы по кибербезопасности НАТО. Имеет степень магистра от Военно-морского училища-аспирантуры в г. Монтерей, штат Калифорния, и степень магистра по специальности «Управление кадрами» от Университета Манчестера, Великобритания.

Капитан Домингос Таварес – заместитель начальника разведслужбы Кабо Верде с 2013 г. После поступления на военную службу в 1997 г. на должность командира артиллерийского взвода, он получил офицерское звание в 2000 г. Имеет степень бакалавра по специальности математика и статистика от Университета Кабо Верде. Закончил офицерские подготовительные курсы в Колледже военной полиции сухопутных сил США в г. Форт Леонард Вуд в штате Миссури, прослушал базовый курс офицера военной разведки для стран Африки в Сенегале и курс по борьбе с терроризмом и пиратством в Центре ВМФ/ВВС США в Пенсаколе, штат Флорида. В Центре им. Маршалла он обучался по программе «Борьба с международной организованной преступностью».

Майор Волбери Ногуейра де Лима Сильва в Вооруженных Силах Бразилии занимает должность штабного офицера в Командовании киберзащиты. С 2012 г. по 2013 г. он служил в должности командира 2-й сигнальной роты., а в 2016 г. занимал должность начальника Подразделения кибероперацій в Центре киберзащиты Бразилии. Волбери был слушателем курсов, организованных Вооруженными Силами Германии и Системой командования и управления НАТО. Он также обучался по «Программе исследований кибербезопасности» в Центре им. Маршалла.

Агниешка Вербитска – эксперт по кибербезопасности, международным отношениям и средствам массовой информации. Она была советником спикеров парламента Польши, президентов Польши и Германии и полномочного представителя министра Польши по вопросам цифровых технологий и кибербезопасности. Вербитска оказывает помощь в реализации директивы Европарламента по вопросам создания сетей и информационных систем, участвовала в разработке киберстратегии Польши и координирует участие польского правительства в Европейской организации кибербезопасности. Она изучала политологию в университетах Варшавы, Констанца и Бонна.

per Concordiam

Журнал по проблемам безопасности и обороны Европы

КИБЕРПРОСТРАНСТВО: ЗАЩИТА КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Том 9, № 1, 2018

Центр имени Маршалла

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

Контактная информация:

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

per Concordiam является профессиональным журналом, публикуемым ежеквартально Европейским командованием США и Европейским центром по изучению вопросов безопасности имени Джоджа 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)

Иллюстрация PER CONCORDIAM

УКРАИНА: *извлеченные уроки*

Российские многоуровневые кибератаки не знают границ

Полковник Виктор Лисаконов, начальник Управления информационного обеспечения при Генеральном штабе Вооруженных сил Украины

Испокон веков инновации двигали вперед военную стратегию. Изобретение пороха, оружия с нарезным стволом и двигателя внутреннего сгорания дали огромный толчок не только военной стратегии, но и всей истории. XX век не был исключением. Развивающийся интернет продолжает расширять возможности информационных технологий. Однако, как и в случаях с другими великими изобретениями, его возможности часто используются во зло. Первые компьютерные вирусы были созданы просто шутки ради, но они послужили предупреждением для одних и началом криминальной деятельности для других — в настоящее время распространены такие явления как компьютерный шпионаж, кибератаки и «кража личности». В то же время у киберугрозы есть и новый аспект.

23 декабря 2015 г. неизвестные хакеры отключили около 30 электроэнергетических подстанций в Украине, оставив без электроэнергии в середине зимы 250 тыс. человек. До той ночи никто никогда не использовал кибератаки на критические объекты гражданской инфраструктуры без очевидных финансовых выгод. Сейчас мы столкнулись с новой угрозой, у которой имеется гигантский военный и геополитический потенциал. За короткий срок простое использование уязвимости систем превратилось в эффективный инструмент гибридных возможностей, при помощи которых достигаются определенные геополитические цели. Это отражает новую оперативную обстановку кибервойны, которая, как продемонстрировала Россия, используется для достижения военного и всеобъемлющего превосходства в настоящих и возможных будущих конфликтах. Понимание угроз, особенно на их начальной фазе, играет чрезвычайно важную роль в выборе эффективных ответных мер.

Печально известная «доктрина Герасимова» появилась в 2013 г., когда в российской еженедельной газете «Военно-промышленный курьер» была опубликована статья начальника генерального штаба России генерала Валерия Герасимова под названием «Ценность науки в предвидении». Эта российская доктрина, примененная в Украине под надзором Владислава Суркова, личного советника президента России Владимира Путина, предполагает создание хаоса, противоречий и внутренних конфликтов. Хотя порождение нестабильности и хаоса при разрешении конфликтов применялось Россией и раньше, Герасимов и Сурков приспособили его под использование в продолжающейся гибридной агрессии против Украины. Применение киберсредств в сочетании с мощной пропагандистской основой, политическим давлением и широкомасштабным применением военной силы было достаточно эффективным, чтобы породить нестабильность в Украине.

Начиная с аннексии Крыма, на всем протяжении росийско-украинского конфликта на востоке Украины, кибероперации сопровождали все этапы агрессии, особенно военные операции. В своей книге «Кибервойна в перспективе: российская агрессия против Украины» Кеннет Гирз дает следующее объяснение: «В Украине Россия экспериментирует, как лучше достичь военных и политических выгод при помощи кибероперацій». В своей работе «Кибервойна и стратегическая культура: российская интеграция кибервозможностей в генеральную стратегию» Джеймс Виртц

Российские военные без опознавательных знаков, известные как «зеленые человечки», двигаются в сторону военной базы Перевальное, Украина, после вторжения на принадлежащий Украине Крымский полуостров. Март 2014 г. GETTY IMAGES

описывает роль киберпространства в российской стратегии следующим образом: «Похоже, что Российская Федерация разработала возможность интеграции кибервойны в глобальную стратегию, способную достигать политических целей». При этом эксплуатируются такие обстоятельства, как отсутствие международных правовых норм в этой области, сложность кибернетической сферы и присущая кибератакам анонимность. Такой подход позволяет проводить любые наносящие вред кибероперации, при этом почти не оставляя никаких следов или доказательств российского присутствия.

На протяжении четырех лет российской агрессии, Украина находилась под постоянным давлением кибератак почти во всех сферах жизни. Однако, нападения на объекты критически важной инфраструктуры превратились в одни из наиболее опасных и эффективных в плане социальных последствий. Семнадцать лет назад эксперт в области безопасности Брюс Шнейер в своей книге «Секреты и обманы: кибербезопасность в мире компьютерных сетей» описал изменение парадигмы, состоящее в массированном применении гражданских технологий и инфраструктуры для военных целей вместо привычных военных средств. Использование одних и тех же компьютерных систем гражданскими и военными пользователями предполагает, что нападения могут совершаться как против гражданских, так и против военных объектов. Учитывая то, что произошло в Украине, становится очевидным, что нападения на объекты критически важной инфраструктуры представляют сегодня одну из наиболее серьезных опасностей.

Бюрократические трудности

Возможно, самой большой проблемой, касающейся нападений на критически важные объекты инфраструктуры, является несовершенство международного права в части кибербезопасности и коллективной обороны. В связи с относительной новизной кибернетической сферы, отсутствует необходимая законодательная база или контрольный механизм, позволяющие наказывать киберпреступников. Действия противников требуют подобающего и пропорционального ответа; однако, действующего механизма для принятия таких ответных мер в настоящее время не существует.

Статья 5 Устава НАТО предполагает, что на агрессию против одного из партнеров последует ответ всех партеров, включая возможное использование военной силы. С июля 2016 г. альянс начал признавать киберпространство такой же сферой проведения операций, как и воздух, земля и вода. Это означает, что нападение на любого из союзников в киберпространстве дает основание для ответных действий, возможно даже военного характера. Однако, когда речь идет о кибератаках, очень трудно и сложно доказать их первоисточник. Как вы сможете доказать, что нападение совершил именно тот, кого вы подозреваете? Какие именно будут необходимы доказательства? Какой вид нападения может потребовать

военного ответа со стороны всей организации? Имеются ли у НАТО разработанные процедуры для реагирования на такие ситуации? Варианты ответных мер, скорее всего, существуют, но любое решение может быть заблокировано одним или несколькими членами организации. Тут больше вопросов, чем ответов. Вот почему на протяжении примерно последних десяти лет кибернападений на критически важные объекты инфраструктуры в периоды геополитической конфронтации (начиная с серии массированных нападений в 2007 г. на институты государственного и частного сектора в Эстонии) так и не было ни одного веского прецедента, когда бы официально была названа нападающая сторона или приняты меры наказания против нападавшего.

Такое отсутствие ясности способствует росту количества кибератак, и некоторые государства успешно используют эту неопределенность для достижения своих геополитических и военных целей. И хотя мы традиционно под критическими объектами инфраструктуры подразумеваем гражданские объекты, хакеры не будут делать различия между гражданскими и военными целями. Иными словами, скорее всего, кибернападения на критически важные объекты, независимо от того, относятся ли они к гражданской или военной категории, будут продолжаться.

Кроме того, системы глобальной безопасности основываются на скоординированных ответах на акт агрессии. Это означает, что международный орган, отвечающий за вопросы безопасности, обсуждает проблему, затем голосует за предлагаемые ответные меры, после чего эти меры реализуются. На каждый из этих шагов затрачивается чрезвычайно важный ресурс: время. Учитывая природу и назначение критически важных объектов инфраструктуры, такой длительный срок подготовки ответных мер может дорого стоить — может разразиться гуманитарная или экологическая катастрофа, в результате которой погибнут невинные люди и будет нанесен ущерб окружающей среде. Такие потенциально катастрофические последствия требуют обязательных изменений в процедурах принятия ответных мер.

В соответствии с законами ведения войны, определенными Женевскими конвенциями (и впоследствии Дополнительным протоколом к Женевским конвенциям от 12 августа 1949 г. и Протоколом I от 8 июня 1977 г.), любые нападения на объекты гражданской инфраструктуры строго запрещены. Эти правила предполагают, что нападения на гражданскую инфраструктуру включают и кибернападения, хотя это пока и не прописано в Женевских конвенциях. Потенциальная анонимность таких нападений в кибернетической сфере вместе с несовершенством правовых норм дают отдельным группировкам и даже государствам возможность беспрепятственно действовать в киберпространстве, не неся при этом наказаний или правовых последствий. Самый опасный сценарий предполагает нападение на критически важные объекты гражданской инфраструктуры с целью достижения военного превосходства.

Рост количества кибератак

После «возрождения» Вооруженных сил Украины, которое включало значительный рост оборонных возможностей и стабилизацию ситуации на линии фронта, российские кибератаки стали носить более отчетливый характер — их целью является оказание давления гибридного характера на Украину. Еще недавно почти никто не мог себе представить меры по развалу транспортной инфраструктуры или отключения электричества в городской сети в качестве средств достижения геополитических целей. До этого представляли угрозу только террористические нападения на критически важные объекты инфраструктуры с использованием импровизированных взрывных устройств или аналогичных конвенциональных средств. Но сейчас во время геополитического противостояния реальностью стали нападения на критическую инфраструктуру при помощи кибернетических средств. За последние два года критические объекты инфраструктуры Украины не менее десятка раз подвергались нападению.

Наиболее показательными примерами таких нападений являются отключение электроэнергии в городских масштабах в Киеве, нападение на энергосеть в западной Украине, нападение на Министерство финансов Украины и администрацию железных дорог, и, конечно же, нападение с использованием вируса NotPetya. Стоит отметить, что объектами всех этих нападений стали гражданские институты, а не правительственные или военные цели. Задача состояла в том, чтобы усложнить повседневную жизнь простым гражданам, заблокировав им доступ к банкоматам, сорвать ведение деловых операций и т.д. Например, хакерские атаки на Министерство финансов и администрацию железных дорог привели к значительным финансовым потерям и задержкам в движении транспорта. Правительство практически не понесло никакого финансового ущерба, но простые люди испытывали проблемы, не имея возможности приобрести билеты или снять деньги в банке в период новогодних праздников. Эти попытки дестабилизации были нацелены на деморализацию и подрыв украинского общества изнутри.

Нападение с применением вируса NotPetya было массированной кампанией, отразившейся на всей стране, поскольку оно привело к финансовым потерям, приостановке работы транспортной системы, запугиванию населения и утечке информации. Тщательный анализ выявил сложную и многоуровневую природу этого нападения с высокой степенью применения кибертехнологий. Этот чрезвычайно высокий уровень сложности и многоуровневая природа свидетельствовали о государственной поддержке этой вирусной атаки. Кампания была не просто актом шпионажа или операцией с целью нанести финансовый ущерб или психологическую травму. Это был практический акт использования кибервойны в качестве основного компонента проведения гибридной операции, что, в свою очередь, является реализацией «доктрины Герасимова». Из кампании с использованием вируса NotPetya можно сделать следующий вывод — доминирование в кибервойне играет чрезвычайно важную роль

в достижении превосходства в этой геополитической конфронтации.

В соответствии с «доктриной Герасимова», Россия интенсивно разрабатывает и широко применяет наступательные кибервозможности. Основная часть этих возможностей направлена на критически важные объекты инфраструктуры с целью нанести вред обычным людям, сделать их жизнь более тяжелой и создать атмосферу массового недовольства. Главная задача состоит в использовании доминирующей позиции в кибервойне для получения преимуществ в геополитических столкновениях. Подходы, использованные в Украине, могут быть, и, возможно, будут использованы против других геополитических оппонентов России. В этой связи одним из основных приоритетов является защита ключевых объектов инфраструктуры от кибернападений. К этому еще добавляется проблема подготовки простых граждан к тому, что в случае геополитической конфронтации они почти стопроцентно станут мишенью.

Возрастающая жестокость и изощренность

Концепцию использования кибератаки против европейского государства следует оценивать с позиции эффективности для достижения геополитических целей. Количество, жестокость и изощренность таких нападений возрастают. Например, во время российско-грузинской войны в августе 2008 г. для того, чтобы сорвать коммуникации между правительством Грузии и гражданами страны, российские военные кибергруппы использовали преимущественно низкотехнологичные вирусные атаки «Отказ от обслуживания» (DDoS-атаки). Шесть лет спустя во время российской оккупации Крымского полуострова гораздо более высокотехнологичные нападения на телекоммуникационные узлы Украины привели к тому, что траффик был перенаправлен на серверы, находящиеся под контролем России. Анализ полученной информации дал российским специалистам преимущество в плане понимания и предвидения шагов Украины в последующих военных операциях.

Кроме того, хакеры довольно успешно разорвали целевые линии коммуникаций между украинскими активистами и международными ресурсами, чтобы изолировать страну от международных платформ. После начала «горячей фазы» российская тактика стала более изощренной, и все чаше объектом кибернападений становиться критически важная военная инфраструктура. Начались они с «детских» атак (когда неопытные хакеры используют программы, написанные другими) на ключевые военные компьютерные сети и постепенно дошли до хорошо организованного крупного фишинга (объектами нападения стали богатые, влиятельные или известные люди) и социальной инженерии (психологические манипуляции с целью заставить объект непреднамеренно выдать закрытую информацию) против высокопоставленных офицеров. Также стоит отметить непрекращающиеся кампании кибершпионажа, которые быстро приобрели высокую степень изощренности и сложности. Кампания под названием операция «Армагеддон», начавшаяся в 2013 г., представляла собой попытку шпионажа с целью сбора чувствительной информации. Вышеупомянутая кампания NotPetya содержала широкий набор инструментов и приемов, включая замену действительного обновления программ финансовых институтов на программы, зараженные вирусами, требования выкупа и удаление информации. Учитывая ситуацию в Украине, трудно переоценить последствия утечки информации. Как правило, эти атаки не нацелены на конкретные институты в военном, государственном или частном секторах. Таким образом, смягчение отрицательных последствий этих нападений является наиболее эффективным ответом, для чего должны предприниматься скоординированные усилия на правительственном уровне.

Что касается военной сферы, то украинские специалисты, отвечающие за киберзащиту, также отметили возросшую настойчивость и изощренность нападений (использование уязвимости конкретного объекта, многовекторность нападений, кастомизированные сложные вирусы, атаки «нулевого дня» и т.д.) против военных объектов и критически важных объектов гражданской инфраструктуры. Снижение уровня таких угроз требует не только внедрения комплексной и многоуровневой защиты, но также и сотрудничество между «защитниками», включая гражданские службы, обеспечивающие защиту критических объектов инфраструктуры. Для того, чтобы организовать такое сотрудничество на государственном уровне, необходимо перестроить всю систему обмена информацией между правительсвенными учреждениями и частным сектором.

За последние несколько лет отмечен рост количества и уровня изощренности кибератак против критически важных объектов военной и гражданской инфраструктуры. Эта проблема является движущей силой изменений в системе кибербезопасности всей критически важной инфраструктуры. В этих целях координация кибербезопасности единой государственной организацией была бы наиболее эффективным решением.

Меняющаяся угроза

Анализ нападений на украинские критически важные объекты инфраструктуры обнаружил еще одну интересную тенденцию. Все большее количество атак не приносят нападавшим каких-либо значительных финансовых выгод. Что более важно, эти нападения имеют политический резонанс, социальные последствия (нарастание тенденций протеста, появление чувства симпатии к агрессору) и снижают уровень военных возможностей (сбои в работе линий телекоммуникаций и нарушение режима конфиденциальности закрытых линий связи). Это означает, что изменение вектора атак достигает желаемых результатов, а именно обеспечивает создание преимуществ, способствующих достижению геополитических целей. Хакеры-одиночки, занимающиеся, как правило, операциями с целью получения финансовых

Судебно-медицинские эксперты собирают улики на месте взрыва автомобиля, в результате которого погиб офицер военной разведки полковник Максим Шаповал. Преступление произошло в тот день, когда началась кампания с применением вируса NotPetya. РЕЙТЕР

Во время поминальной службы в Киеве украинский мальчик смотрит на фотографию своего отца – солдата, погибшего в войне с поддерживаемыми Россией сепаратистами. 2017 г. АССОШИЭЙТЕД ПРЕСС

выгод, не в состоянии разработать и осуществить кибероперации на высоком уровне. По этой причине считается, что кибератаки против критически важных объектов украинской инфраструктуры перешли с уровня хакеров-одиночек на уровень организованных групп очень опытных киберэкспертов, скорее всего, пользующихся российской государственной поддержкой.

Последние несколько лет характеризовались появлением постоянной повышенной угрозы (ППУ) со стороны групп опытных экспертов-программистов, пользующихся государственной поддержкой и способных создавать сложное кибероружие. Например, «Совместный аналитический доклад» ФБР о кибератаках во время выборов в США в 2016 г. назвал в качестве вероятных преступников две хорошо известные российские группы, ассоциирующиеся с киберугрозой (ППУ 28 и ППУ 29). Эти группы постоянно и целенаправленно работают над похищением разведданных для российского правительства. Большинство кибероперации против украинских критически важных объектов инфраструктуры в последние несколько лет, скорее всего, было спланировано и осуществлено именно этими группами. Они неоднократно выбирали объектами своих нападений украинские, европейские и американские правительственные институты, такие как военные учреждения, международные организации, «мозговые тресты», СМИ и другие цели, тесно связанные с российскими геополитическими интересами и приоритетами. Основная цель таких групп состоит в создании и поддержании благоприятной для России геополитической ситуации, которая, вместе с украденной информацией, используется российскими властями во время военных операций или политических переговоров.

За последние годы произошло смещение угрозы с отдельных хакеров, нападавших на финансовые институты, на хорошо организованные и поддерживаемые государством группы профессионалов, атакующих критически важные объекты. Это смещение оказало серьезное влияние на ориентацию, приоритеты и возможности систем кибербезопасности. Всего лишь пару лет назад финансовые институты и богатые корпорации были наиболее прибыльными объектами нападений опытных хакеров. Сегодня же чаще всего нападения осуществляются на военные учреждения и критически важные объекты инфраструктуры.

Жертвами Кампании Фишинга Стали 39 Стран

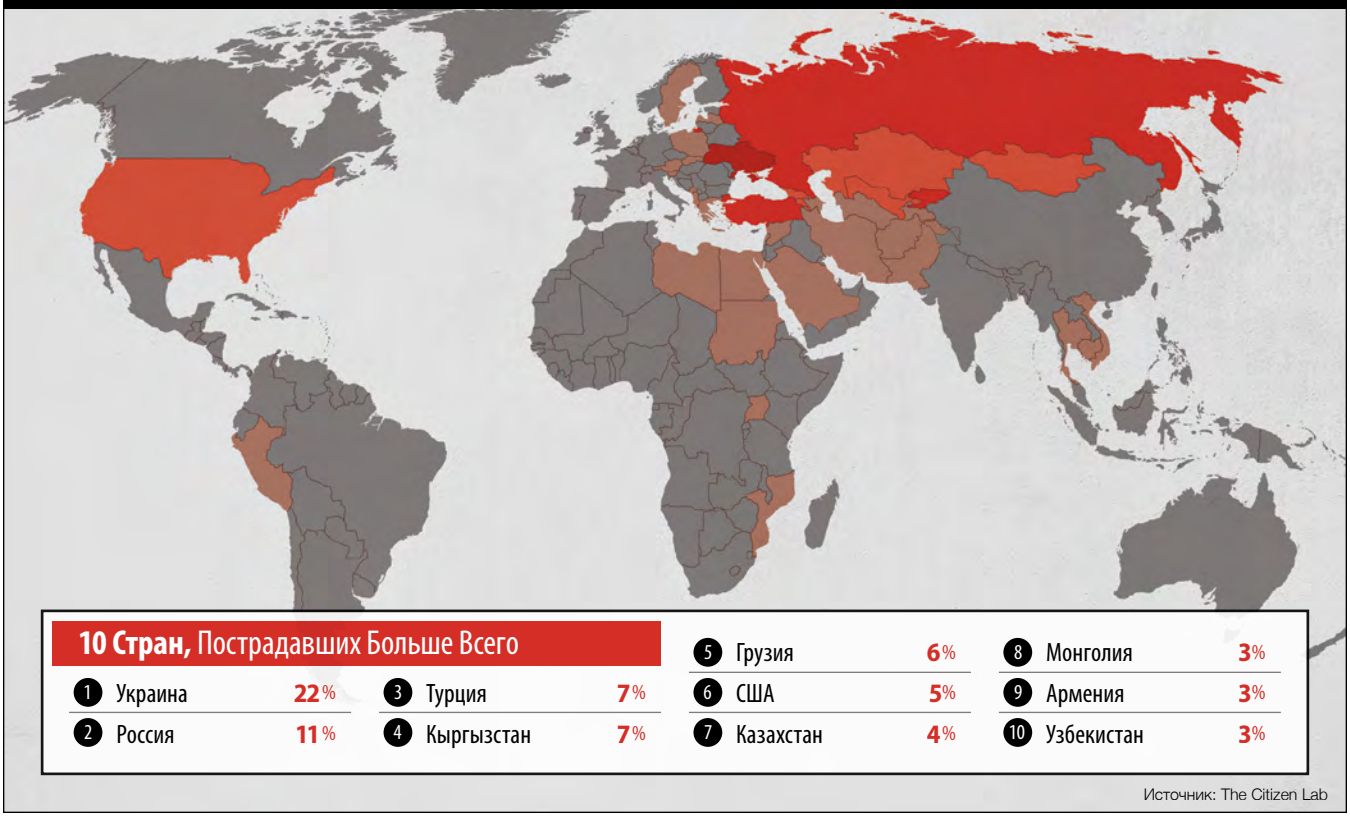


ИЛЛЮСТРАЦИЯ PER CONCORDIAM

10 Стран, Пострадавших Больше Всего

1	Украина	22%	3	Турция	7%	5	Грузия	6%	8	Монголия	3%
2	Россия	11%	4	Кыргызстан	7%	6	США	5%	9	Армения	3%
						7	Казахстан	4%	10	Узбекистан	3%

Источник: The Citizen Lab

В результате массированной кампании фишинга, за которой, как подозревают, стояла Россия, было украдено более 200 адресов электронной почты в 39 странах мира. В дальнейшем эти адреса использовались для манипулирования данными и размещения дезинформации.

Синергетические кибератаки

Еще одна серьезная проблема, о которой стоит упомянуть — это синергетическое использование различных типов инструментов конфликта. Синергетический подход предполагает осуществление нападений, скоординированных по времени, месту и целям, с тем, чтобы усилить эффект каждого отдельного нападения. Этот подход не нов, и Россия уже успешно использовала его в Грузии. В своей статье «Исследование конкретного случая кибервойны: Грузия 2008 г.» Дэвид М. Холлис описывает это как «первый случай в истории, когда скоординированные нападения в киберпространстве были синхронизированы с крупными военными действиями в других сферах ведения войны». Однако, сфера кибернетики и ее безграничность и анонимность добавляют еще одну переменную в уравнение в свете российской агрессии против Украины. Российская аннексия Крыма началась с целого ряда дезинформационных кампаний, имевших целью создать ситуацию неопределенности и подавленности и оттянуть ответные действия Украины. Огромные армии троллей создали впечатление сильной поддержки российских действий со стороны населения Крыма, и та же самая картина передавалась на международную аудиторию по спонсируемым Россией международным телеканалам, таким как «Россия сегодня» и «Спутник». Одновременно с этим, чтобы обеспечить информационное превосходство, российский спецназ физически уничтожил кабельные соединения с материковой частью Украины и захватил пункты передачи информации по интернету.

Во время вторжения в Донбасс Украина столкнулась с гораздо более сложным и изощренным нападением. До начала «горячей фазы» конфликта российские кампании разведки и шпионажа подготовили очень благотворную почву для будущих военных операций против Вооруженных Сил Украины. Благодаря этому преимуществу, кибератаки, электронная борьба и психологические и информационные операции были хорошо скоординированы с мощными военными ударами. Такое синергетическое использование различных средств и методов из различных сфер повышало степень воздействия и часто приводило в замешательство атакуемые украинские боевые подразделения. Например, во время российского наступления на Дебальцево и захвата донецкого аэропорта российские специалисты систематически посылали деморализующие текстовые сообщения украинским солдатам и их семьям. Кроме того, против командно-контрольной инфраструктуры были предприняты массированные DDoS-атаки, а тактические радиокоммуникации были прерваны российскими средствами электронной борьбы. «Во время 240-дневной осады донецкого аэропорта русские специалисты смогли перекрыть системы спутниковой навигации, а также сигналы радио и радаров. Их возможности электронного перехвата были

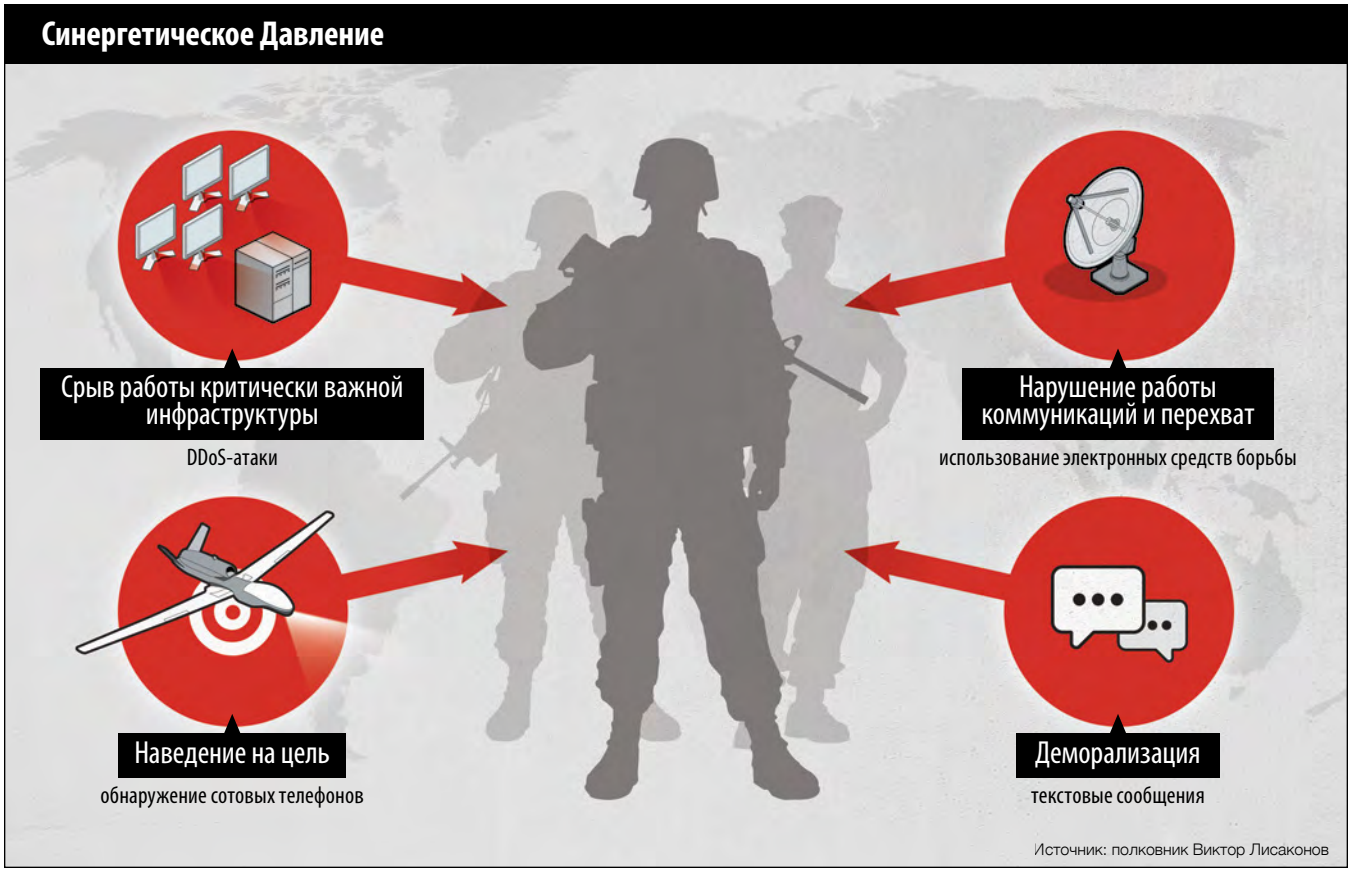


ИЛЛЮСТРАЦИЯ PER CONCORDIAM

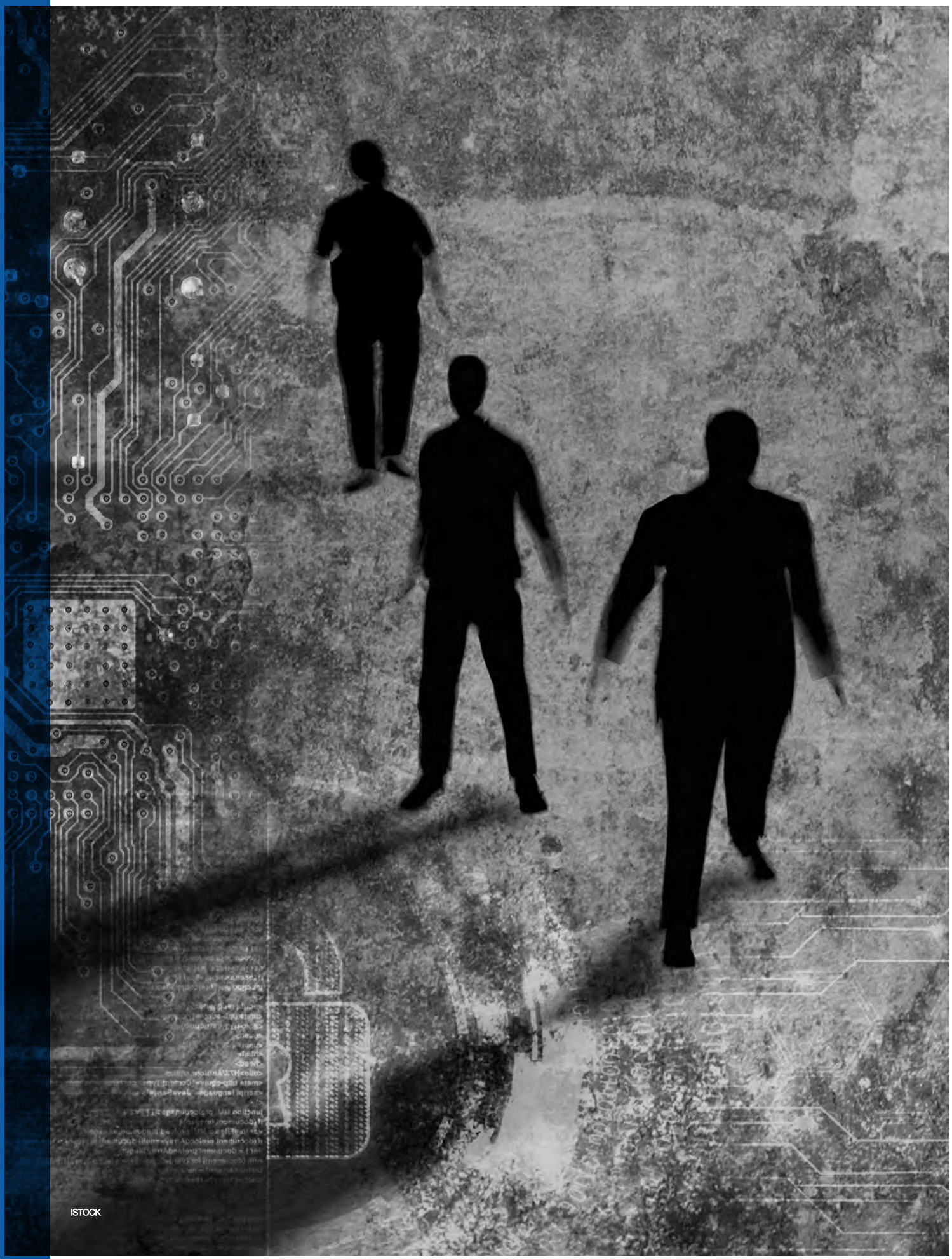
Во время крупных российских операций украинские военные становятся объектами сложного многовекторного воздействия, включающего электронные средства борьбы и кибермеры психологического характера.

настолько велики, что украинская сеть коммуникаций была просто парализована», — пишет Роберт Х. Скейлз в своей статье «Новое супероружие России». Все вышеупомянутые действия дополнялись традиционной мощной пропагандой. Социальные сети были полны дезинформации и панических сообщений. Сотни ботов из фабрик троллей и пророссийски настроенных граждан атаковали украинское правительство и распространяли лживые истории о сотнях, а иногда и тысячах украинских солдат, убитых в боях или попавших в плен.

Эта многоуровневая операция была скоординирована по времени, объектам нападения и поставленным задачам. Сочетание кибернетической сферы, средств электронной борьбы, психологических и информационных операций с одновременными боевыми действиями нанесли оборонным усилиям Украины серьезный ущерб. Принимая во внимание внутреннюю политическую ситуацию в Украине и отношения на международной арене, синергетическое использование такого широкого набора инструментов было наиболее эффективной стратегией. Однако, самым опасным аспектом такого подхода является то, что он глобален по своим масштабам и может быть использован с такой же эффективностью против любого геополитического оппонента.

Заключение

Автор этой статьи и его коллеги непосредственным образом участвуют в усилиях Украины, направленных на противостояние такой гибридной агрессии со стороны России. «Доктрина Герасимова» предполагает широкое использование гибридных средств против противника с целью создания нестабильности и внутреннего конфликта, как это и было проделано в случае с Украиной. Объекты критически важной инфраструктуры являются наиболее выгодными мишенями для такого подхода. За последнее десятилетие российские наступательные кибервозможности прошли эволюцию от простых единичных атак, которые потом отрицались, до сложных многоуровневых операций, которые объединяют одновременное и скоординированное использование психологических, электронных и чисто военных компонентов, а также финансовое и международное давление. Проблема сегодняшней обстановки в том, что ни общество, ни законодательные структуры до конца не понимают всю опасность этих наступательных операций и поэтому не реагируют на них должным образом. Этот сложный гибридный подход потенциально может иметь катастрофические последствия для критически важных объектов инфраструктуры и окружающей среды. Такие нападения порождают в обществе дезорганизованность, неопределенность и нестабильность, которые могут создавать дополнительное давление на принимающих решения высокопоставленных лиц, что даст нападающей стороне геополитические преимущества. □



ISTOCK

ГЛАВНОЕ — ЖИЗНЕСТОЙКОСТЬ

Как противостоять известным и неведомым опасностям

Подполковник д-р Дарко Галинец, Министерство обороны Республики Хорватия | Фотографии Ассошиэйтед Пресс

Военная терминология может употребляться в невоенной тематике точно так же, как военные технологии могут быть применимы в гражданских областях (например, сеть Агентства передовых исследовательских проектов со временем превратилось в интернет). Во многих случаях такое перемещение терминологии приносит пользу, поскольку оно привносит больше специфики в обсуждение функционирования технологий. Однако, полезность термина снижается, если его четкое значение размывается или теряется при переходе в новый контекст. Возьмем, к примеру, кибербезопасность, которой уже более десятилетия занимаются военные круги. В последние годы этот термин стал появляться в целом ряде других контекстов, многие из которых имеют мало или вообще ничего общего с первоначальным значением этого термина. Его неправильное использование понижает важность практических шагов, которые делают кибербезопасность термином, охватывающим такие относящиеся к цифровым операциям сферы, как информационная безопасность, безопасность операционных технологий (ОТ) и безопасность информационных технологий (ИТ).

В такой же степени важно дать точное определение и термину киберзащита. В контексте специфической среды киберзащита анализирует возможные угрозы и помогает разрабатывать и реализовывать стратегии, необходимые для противодействия злонамеренным атакам или угрозам. В плане защиты потенциального объекта нападения или реагирования на существующие угрозы киберзащита охватывает целый круг мер. В число таких мер входят: действия, делающие среду менее привлекательной для нападающего; определение критически важных объектов и информации; введение в действие средств превентивного контроля, которые сделают нападение дорогостоящим предприятием; ответное обнаружение; и усиление возможностей реагирования и ответных мер.

Определение термина кибербезопасность

В 2016 г. в своей статье в журнале «World Economic Forum» Дэниел Добрыговски дал следующее определение: «Кибербезопасность — это регулирование, развитие, управление и использование информационной безопасности и безопасности ОТ в целях обеспечения соблюдения установленных норм, а также защиты собственных сетей и взлома сетей противника». По мнению экспертов, кибербезопасность:

- Это термин, охватывающий действия по обеспечению безопасности ИТ, информационной безопасности, безопасности ОТ и безопасности наступательных операций (см. рис. 1).
- Использует инструменты и приемы обеспечения безопасности ИТ, безопасности ОТ и информационной безопасности для того, чтобы минимизировать уязвимость, поддерживать целостность системы, давать доступ только утвержденным пользователям и защищать сети.
- Включает в себя разработку и использование ИТ и ОТ для осуществления нападений на противников.
- Поддерживает цели сохранности информации в пределах цифрового контекста, но не участвует в обеспечении безопасности аналоговых медиа (например, бумажных документов).

В то же время кибербезопасность это не:

- Просто синоним понятий информационная безопасность, безопасность ОТ или безопасность ИТ.
- Использование информационной безопасности для защиты предприятия от преступлений.

Безопасность работы с цифровыми технологиями

Рис. 1

Источник: Gartner, Inc. (2018)

- Кибервойна (эксперты сходятся во мнении, что термин «кибервойна» относится к использованию возможностей кибербезопасности в контексте состояния войны, хотя это сложная область, и ее не стоит путать с физическими нападениями на инфраструктуру с разрушением собственности и механизмов, и с информационной войной, предполагающей использование психологических операций при помощи приемов пропаганды и дезинформации).
- Кибертерроризм (подобно кибервойне, кибертерроризм предполагает использование приемов обеспечения кибербезопасности в ходе террористической кампании или деятельности).
- Киберпреступления (это просто термин для определения преступных нападений с использованием инфраструктуры ИТ и не имеет никакого отношения к кибербезопасности).

Правильное использоание кибербезопасности:

- Когда, принимая ответные меры по оценке риска угрозы, предприятие увеличивает инвестиции в кибербезопасность с целью снизить уязвимость и повысить возможности контратаки против установленной нападающей стороны (интеграция безопасности ИТ и возможностей наступательных действий в рамках единой программы).
- Когда для обеспечения более комплексного ответа на угрозы происходит интеграция программ обеспечения безопасности ИТ и ОТ в рамках одной группы кибербезопасности.
- Когда организация хакеров-активистов «Аноним» использует целый ряд приемов обеспечения кибербезопасности для достижения своих целей (использование наступательных возможностей).

Примеры ненадлежащего использования кибербезопасности:

- Чтобы снизить вероятность кражи ноутбуков план кибербезопасности магазина призывает к использованию шифрования компьютерных дисководов целиком (это является базовой мерой в плане безопасности ИТ).
- Политика в области кибербезопасности требует использования сложных паролей для всех производственных систем на предприятии, которые функционируют с участием компьютера (это является базовой мерой в плане безопасности ОТ).

Определение термина кибероборона

Согласно оценкам Центра мастерства совместной кибероборонны НАТО, не существует единых определений в «кибер»-терминологии — люди в разных странах и даже в разных организациях подразумевают под этими терминами разные вещи, несмотря на то, что они часто используются в ведущих средствах массовой информации и в заявлениях национальных и международных организаций.

Однако, techopedia.com дает кибероборонe следующее определение: «Кибероборона — это защитный механизм компьютерных сетей, который включает ответные меры на определенные действия, защиту критически важной инфраструктуры и сохранение информации для организаций, правительственных учреждений и других возможных обладателей компьютерных сетей. Основное внимание кибероборона уделяет предотвращению, обнаружению угроз и принятию своевременных ответных мер на нападения или угрозы с тем, чтобы предотвратить вмешательство в функционирование инфраструктуры или манипуляцию информацией. По мере роста количества и сложности кибернападений кибероборона становится жизненно необходимой для большинства объектов, стремящихся ограничить доступ к информации и материальным активам».

Кибероборона дает крайне необходимые гарантии нормального проведения всех процедур и операций, не опасаясь угроз. Она позволяет повысить использование стратегии безопасности и соответствующих ресурсов с максимальной эффективностью. Кибероборона также помогает повысить эффективность использования ресурсов безопасности и затрат на безопасность, особенно на критических объектах.

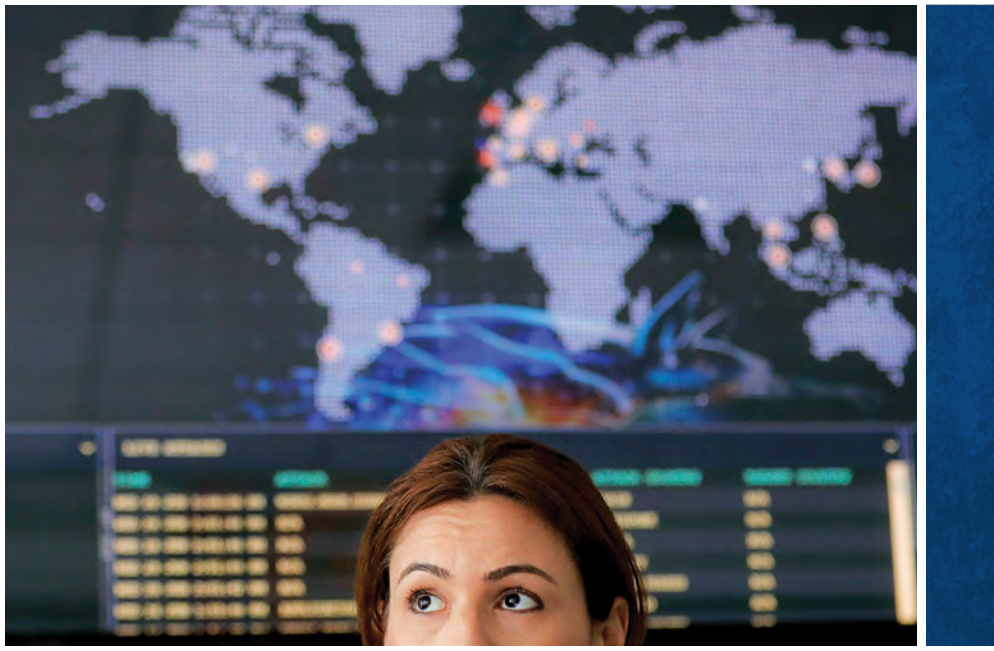
Признавая необходимость ускоренного обнаружения нападения и принятия ответных мер

против нападающей стороны, Министерство обороны США в качестве принимаемых в режиме реального времени синхронизированных мер по обнаружению и распознаванию нападения, его анализу и снижению степени угроз и уязвимости разработало новую концепцию — концепцию активной кибероборонны.

В то время как стоимость защиты киберструктур, а также и совокупность потерь в случае успешного нападения возрастает, стоимость осуществления самого нападения одновременно с этим уменьшается, о чем свидетельствует infosecurity.net.

Однако, в сегодняшнем мире асимметричных войн и быстро меняющихся угроз медицинское определение термина «стратегия», данное в словаре Merriam-Webster, более подходит для определения кибербезопасности: «адаптация или комплекс адаптационных мер (в отношении таких факторов как поведение, метаболизм или структура), которые выполняют или, по-видимому выполняют важную функцию в достижении эволюционного успеха».

Ключ к достижению более высокой степени кибербезопасности состоит в достижении более низкой степени уязвимости. Хотя осознание угрозы играет важную роль, снижение уровня уязвимости затрудняет осуществление любого нападения, как утверждает технологическая исследовательская и консалтинговая компания Gartner Inc.



Женщина в штаб-квартире специализирующейся в вопросах кибербезопасности фирмы Bitdefender в Бухаресте, Румыния, перед картой, показывающей в реальном времени кибератаки в 2017 г. Программа, которую злоумышленники используют для получения выкупа, может парализовать компьютеры по всему миру.

Управление рисками

Взломы системы кибербезопасности, подобные тем, которые имели место в интернет-службе знакомств Ashley Madison, американском Департаменте управления персоналом и банке J.P. Morgan Chase, продемонстрировали, насколько реальна и непосредственна угроза взлома компьютерных систем. Бывший директор Агентства национальной безопасности США и бывший начальник Киберкомандования США адмирал Майк Роджерс вынужден был признать, что «Вопрос не в том, смогут ли они «пробить» вашу защиту, а в том, когда они смогут это сделать».

Если состояние кибербезопасности в организации недостаточно заметно, то такая организация не сможет справиться с рисками для кибербезопасности и почти наверняка станет жертвой взлома. «Заметность состояния кибербезопасности» означает владение полной картиной, которая позволяет дать ответы на следующие вопросы:

- Каковы, в целом по предприятию, нынешние показатели уровней рисков для кибербезопасности от многочисленных угроз?
- Являются ли эти уровни приемлемыми?
- Если нет, то в чем состоит взвешенный и приоритизированный план действий по снижению уровней рисков до приемлемых?
- От кого именно исходят угрозы и насколько срочно необходимо реагировать на риски?

Способность определить показатель состояния кибербезопасности является принципиальным вопросом; если его невозможно измерить, то это значит, что успешное управление рисками невозможно. Инциденты в сфере безопасности и управление событиями (ИБУС), а также аналитическая работа с информацией могут дать ценные сведения о том, где именно в компьютерной сети организации находятся или могут находиться слабые места. Однако, полной картины они не дают: они являются индикаторами общего состояния рисков, но не дают конкретных количественных характеристик.

Аналогичным образом, разведслужба, занимающаяся угрозами, может определить потерю информации и может дать ценные сведения относительно имевших место или грозящих нападений, но опять-таки, они не являются четкими измерениями состояния рисков. То же самое можно сказать и в отношении отдельных направлений, таких как соблюдение нормативных требований, уязвимость, тестирование на «пробиваемость» сети и аудиты.

Как считает партнер фирмы Acuity Risk Management Саймон Марвел, только посредством тщательного анализа всех соответствующих индикаторов и конкретных факторов можно разработать общую меру степени риска и заметности состояния кибербезопасности. Когда

существует уверенность в конкретных показателях риска для кибербезопасности, тогда имеется возможность быстро реагировать на события и принимать решения. В целях повышения уверенности:

- Определите неприемлемые риски и составьте четкий и разбитый по приоритетам план действий по улучшению управления с тем, чтобы снизить эти риски до приемлемого уровня.
- Улучшите свое понимание результатов разведки угроз, а также ИБУС и анализа информации для того, чтобы разработать более быстрые и прицельные ответные меры.
- Разработайте основанное на показателях риска обоснование инвестиций в совершенствование систем и служб обеспечения кибербезопасности.

Однако, когда уровень угрозы очень высок и угрозы и механизмы управления рисками претерпевают частые изменения, организация обязательно должна обновлять состояние своей кибербезопасности чаще, возможно, даже ежедневно.

По словам Марвела, в то время, как раньше меры по управлению рисками для кибербезопасности могли пересматриваться раз в год в рамках мероприятий по составлению планов и бюджета, сегодня это работающий в режиме реального времени важный помощник в борьбе против взломов компьютерных систем. Взломы систем обеспечения кибербезопасности происходят тогда, когда люди, установленные процедуры, технологии или другие компоненты системы управления рисками для кибербезопасности либо отсутствуют, недостаточны, или по какой-то причине не выполняют свою функцию. Именно поэтому необходимо понимать работу всех важных компонентов системы и механизм их взаимодействия.

Например, это не означает, что система управления рисками должна отслеживать детали работы каждого конечного устройства и статус каждого слабого места в сети, поскольку есть другие инструменты, которые сделают эту работу. Но система управления рисками обязана знать, что все конечные устройства прошли (и продолжают регулярно проходить) идентификацию и, что все критически слабые места в системе быстро устраняются.

В конечном счете, успех в обеспечении кибербезопасности является ничем иным, как результатом процесса эффективного управления рисками. Однако, этот процесс сталкивается со значительными трудностями, связанными с присущей компьютерным системам сложностью, у которых в компонентах и протоколах имеются слабые места, а также с возрастающей изощренностью взломщиков, за которыми зачастую стоят криминальные структуры с обширными ресурсами, а иногда и государства.

Жизнестойкость компьютерных сетей

Учитывая высокий уровень неопределенности и большое количество случаев нападений, совершенно необходимо всемерно способствовать повышению жизнестойкости компьютерных сетей. Жизнестойкость компьютерных сетей — это способность системы, организации, миссии или бизнеса предугадывать давление или нападения на необходимые для функционирования киберресурсы, противостоять им, восстановиться после нападения и приспособить свои возможности к дальнейшим возможным нападениям и давлению. Впервые о жизнестойкости компьютерных сетей заговорили в 2012 г. на Всемирном экономическом форуме в Давосе, Швейцария, и с тех пор эта тема стала приобретать все большую важность для отдельных людей, для бизнес-сообществ и обществ в целом и превратилась в концепцию, на которую все больше обращают внимание и все чаще используют. Об этом свидетельствует академический труд «Жизнестойкость компьютерных сетей — основы для определения».

С точки зрения функционирующей организации, жизнестойкость компьютерных сетей означает способность продолжать выдавать ожидаемый результат, несмотря на попытки противника сорвать работу системы. Понятие «беспрерывность» предполагает, что способность выдавать предполагаемый результат будет сохраняться, даже когда обычные механизмы достижения этого результата вышли из строя в результате кризисной ситуации или после взлома компьютерной сети. Это понятие предполагает способность восстанавливать обычный механизм получения результата после неблагоприятных событий, а также способность постоянно изменять или модифицировать механизм получения результата в ответ на постоянно меняющиеся риски. Предполагаемый результат — это тот, который анализируемый объект (государство, отдельная организация или система ИТ) предполагает получить, например, определенные цели бизнеса или бизнес-процесса или услуги, предоставляемые службами в режиме онлайн.

По своей природе кибербезопасность — многогранная проблема, которая будет продолжать эволюционировать с такой же скоростью, с какой происходит развитие технологий. «11-й Ежегодный обзор глобальной информационной безопасности» указывает на то, что топ-менеджеры убеждены в надежности своих нововведений в сфере компьютерной безопасности. 84% генеральных директоров и 82% директоров ИТ убеждены в эффективности своих программ обеспечения кибербезопасности, в то время, как 78% директоров управлений информационной безопасности выражают полную уверенность в надежности своих существующих программ компьютерной безопасности. Однако, по мере роста количества взломов компаниям следует обращать основное внимание не только на кибербезопасность, но и на жизнестойкость компьютерных сетей. Из года в год количество зарегистрированных инцидентов в сфере кибербезопасности значительно возрастает — от 2 989 случаев в 2012 г. до 3 741 в 2013 г. Кроме того, за этот же период средние потери на один инцидент возросли на 23%, а количество организаций, заявивших о потерях более чем в 10 млн. долл. США за один инцидент, в период с 2012 по 2014 г., по данным журнала «Forbes», возросло на 75%.

Кибербезопасность не решает всех задач обеспечения безопасности, поэтому больше внимания необходимо

уделять аспекту жизнестойкости компьютерных сетей. Если компания осознает, что против нее будет предпринята кибератака, и эта кибератака будет успешной, то она должна тут же перейти к следующему шагу — внедрению программы обеспечения жизнестойкости компьютерных сетей. Согласно определению, данному журналом «Forbes», такая программа охватывает как защиту от нападений, так и их предотвращение, но при этом основной упор делает на ответные меры и жизнестойкость в моменты кризиса.

«Вопрос не в том, смогут ли они «пробить» вашу защиту, а в том, когда они смогут это сделать», – считает бывший директор Агентства национальной безопасности США и бывший начальник Киберкомандования США адмирал Майк Роджерс.

Новые риски

Сегодня профессионалы в области компьютерной безопасности борются с угрозами, возникающими как за пределами их организаций, так и исходящими от сотрудников этих организаций. Но как быть с теми угрозами, о существовании которых уже хорошо известно? В течение последующих нескольких лет мы будем свидетелями как самых разнообразных нападений, так и прогресса в технологиях и процедурах, направленных на их предотвращение.

Одной лишь системы кибербезопасности уже недостаточно, необходимы стратегии защиты, предотвращения нападения и принятия ответных мер. Сама идея жизнестойкости компьютерных систем, в ее самом простом виде, представляет собой оценку того, что произойдет до, во время и после того, как система цифровых сетей столкнется с угрозой. Жизнестойкость не стоит понимать как синоним понятия «восстановление». Жизнестойкость не разрабатывается как ответ на какое-то одно конкретное нападение; она создается в течение долгого времени и должна быть включена в общую стратегию компании или организации. Жизнестойкость в контексте способности компаний и организаций выдерживать киберинциденты подразумевает подготовительную работу, проделанную организацией в ответ на выявленные слабые места и угрозы, разработку защитных механизмов и ресурсы, зарезервированные для минимизации последствий отказа системы кибербезопасности. Ключевой момент в этой схеме — нормализация работы после нападения. Компьютерный риск должен рассматриваться так же, как любой другой риск, с которым организация должна бороться, чтобы достичь поставленных целей. Руководители в сфере частного бизнеса и в правительственных структурах должны признавать важность аспекта компьютерной жизнестойкости по двум причинам: во-первых, таким образом они избегают катастрофических последствий, которыми грозит подход к компьютерным рискам по принципу «все или ничего» (когда предотвращение проникновения в систему является единственным планом действий); и во-вторых, при этом в поле зрения попадает более широкий круг вопросов, чем просто безопасность информационных технологий и информационная безопасность, о чем пишет в своей статье Добрыговски в журнале «World Economic Forum».

Первое замечание о том, что долгосрочная перспектива и устойчивость являются ключевыми факторами в обеспечении жизнестойкости компьютерных сетей, не нуждается в дальнейших разъяснениях. План, охватывающий набор действий и результатов до, во время и после возникновения угрозы, как правило, будет более эффективен, чем план, который рассматривает одно конкретное нападение за один раз. Второе замечание о том, что руководители должны расширить круг обсуждаемых вопросов, следует развить несколько шире. Для экономической жизнестойкости и жизнестойкости общества чрезвычайно важно, чтобы мышление специалистов по кибербезопасности выходило за рамки просто информационной безопасности и охватывало жизнестойкость сети в целом, которая могла бы эффективно противостоять как существующим сегодня рискам, так и новым рискам, включающим искусственный интеллект, интернет вещей или квантовые компьютеры. Для обеспечения долгосрочной жизнестойкости компьютерных сетей организации должны включить в свое стратегическое планирование способность приспосабливаться к угрозам, меняющимся по мере быстрого развития подрывных технологий.

В результате развития концепции всеобщей жизнестойкости компьютерных сетей, долгосрочная стратегия (включая прогнозирование, какими технологиями компания будет пользоваться в течение следующих пяти,

Центр НАТО по совместной киберзащите в Таллине, Эстония. Центр считает, что нет единых устоявшихся определений «кибер» -терминов.

десяти или более лет) превращается в постоянные стратегические дебаты, в которые вовлечены как руководители проектов в сфере информационных технологий, так и руководители-стратеги в рамках организации. Принятие концепции жизнестойкости компьютерных сетей обеспечивает более высокую степень готовности и меньшее количество повторений, делая всю систему более рациональной и более эффективной. Безопасность, в отличие от жизнестойкости, может рассматриваться как двоичное понятие. Что-то либо является безопасным, либо нет. Как пишет Добрыговски, зачастую это просто сводится к какой-то одной ограниченной технической функции, которая не разрешает незарегистрированным пользователям вход в сетевую систему.

Хотя существует множество более широких определений кибербезопасности, существует различие между простым контролем за доступом в систему как основой кибербезопасности и стратегическим мышлением на долгосрочную перспективу, порождаемым концепцией жизнестойкости компьютерных сетей. Кроме того, поскольку уязвимое место в какой-то части системы может привести к перебоям в работе всей сети, то жизнестойкость требует того, чтобы в центре дискуссий были системы, а не отдельные организации. Именно поэтому концепцию жизнестойкости лучше всего рассматривать в контексте общественного блага или «общественного достояния». По этой причине очень важны партнерские отношения. Это могут быть как отношения между кампаниями, так и отношения с участием регулирующих органов, прокуратуры и политиков.

Поскольку жизнестойкость компьютерных сетей в конечном счете сводится к управлению рисками, то у нее нет четкой начальной и конечной точки. Она зарождается из разработок стратегий и стремления к тому, чтобы те механизмы передачи рисков, которые работают в случае более традиционных угроз, работали также и в контексте новых кибер-угроз. Ответственность за жизнестойкость компьютерных сетей является скорее вопросом общей стратегии, чем каких-то специфических тактических действий. Обеспечение жизнестойкости системы требует от высшего руководства компании, организации или правительственного учреждения признания важности избегания и уменьшения рисков. Как отмечает Добрыговски, хотя сотрудничество с целью обеспечения более высокой степени жизнестойкости компьютерных сетей является ответственностью всего коллектива, окончательная ответственность лежит все же на руководителях, которые определяют стратегию организации, и именно с них спрашивают, было ли включено обеспечение жизнестойкости компьютерных сетей в общую стратегию организации или нет.

Самая большая угроза для кибербезопасности — неизвестная угроза. Бывший министр обороны США Дональд Рамсфельд во время пресс-конференции в 2002 г. дал следующее объяснение: «Есть известные вещи, которые известны. Это те вещи, которые мы знаем. Есть известные неизвестные. Иными словами, мы знаем, что об этих вещах мы ничего не знаем. И есть также неизвестные неизвестные — мы даже не знаем о том, что каких-то вещей мы не знаем».

Противостояние известным угрозам является необходимой составляющей любой стратегии кибербезопасности. Рядом идут неизвестные угрозы, которые при помощи передовых возможностей предугадываются и перехватываются, и из которых, в конечном счете, извлекаются уроки. Системы имеют различные слабые места и различные процедуры (проблемы), и каждая из них по-своему управляет рисками (решениями). Иными словами, на каждую проблему в сфере безопасности (определенную как известную или неизвестную) имеется соответствующее решение (определенное как известное или неизвестное). Внедряя в модель ценности, полученные во время процесса оценки системы безопасности, мы получаем «известные известные», относящиеся к информационной безопасности, «известные неизвестные», относящиеся к кибербезопасности, и «неизвестные неизвестные», относящиеся к жизнестойкости компьютерных сетей. Эту классификацию дает занимающаяся вопросами кибербезопасности фирма Exclusive Networks.

Пример: есть известный кризис, связанный с персоналом сферы кибербезопасности — недостаток квалифицированных и обученных профессионалов в области безопасности. Но также есть и неизвестное решение

этой кризисной ситуации. Как отмечает журнал «Federal Times», обширный и постоянно растущий масштаб угроз требует соответствующего расширения набора знаний, которыми обладает персонал сферы безопасности, включающий как известные, так и неизвестные знания.

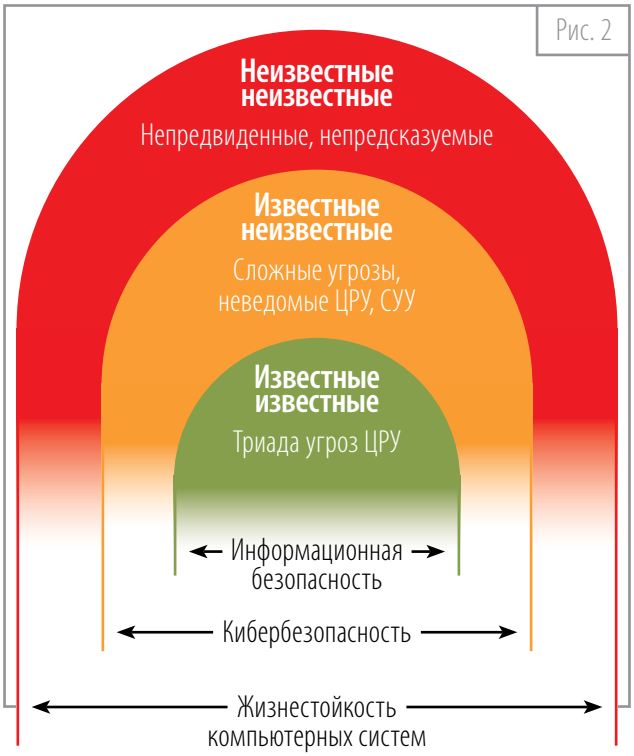
И, наконец, основываясь на знаниях, которые дала автору этой статьи Программа исследований кибербезопасности в Центре им. Маршалла в 2017 г., модельная структура жизнестойкости компьютерных сетей и контент состоит (рис. 2) из информационной безопасности (конфиденциальности, целостности и доступности — триады угроз ЦРУ и ответов на них, т.е. известных известных), кибербезопасности (сложных угроз, неведомых ЦРУ, или современных устойчивых угроз (СУУ) и соответствующих им ответных мер, т.е. известных неизвестных) и жизнестойкости компьютерных сетей (непредвиденных и непредсказуемых угроз и ответов на них — неизвестных неизвестных).

У решений в сфере кибербезопасности есть возможности сделать так, что мы перестанем бояться большого количества неизвестных угроз, сделав их известными. Но будут сохраняться значительные возможности и у тех защитных мер, которые применяются к огромному количеству известных киберугроз, чтобы держать систему постоянно в безопасности. Такой точки зрения придерживается технологическая сервисная компания Exclusive Networks.

Для того, чтобы справляться с растущим количеством угроз, которые сегодня представлены неизвестными неизвестными угрозами, системы стремятся к тому, чтобы дать персоналу возможность создавать новые процедуры, организационные требования и технологии. Создаются технологии, которые, в отличие от традиционных подходов, имеют возможность защитить системы от серьезных угроз путем изучения того, что является «нормальным» для данной организации и ее сотрудников, позволяя выявлять таким образом возникающие аномальные явления. В отличие от традиционных правил и подходов, основанных на наличии подписи для получения разрешения на вход, технологии могут обнаружить угрозы, способные нанести вред организации и ее сети, которые традиционные подходы засечь не в состоянии. Это является ответом на неопределенность и предоставляет организациям адаптивную защиту от угроз как изнутри организации, так и от изощренных кибератак извне.

Модель жизнестойкости компьютерных систем

Рис. 2



Источник: подполковник д-р Дарко Галинец

Заключение

Ни в какой другой области технологическое развитие не имело такой динамичный и всеобъемлющий характер, как в сфере коммуникационных и информационных технологий. В центре внимания всегда были быстрое развитие и внедрение новых услуг и продуктов, в то время как относящиеся к безопасности аспекты, как правило, имели незначительное влияние на широкое принятие новых технологий.

«Срок жизни» современных информационных систем от процесса планирования, введения и использования до прекращения использования очень короток, что часто делает невозможным их систематическое тестирование, которое проводится в виде исключения только в тех случаях, которые этого настоятельно требуют.

Современные общества пронизаны коммуникационными и информационными технологиями. Люди сегодня связываются между собой при помощи различных технологий, передающих текстовые сообщения, изображения и звук, включая растущий сегмент интернета вещей. Отход от предусмотренного функционирования этих взаимосвязанных систем или их отдельных частей больше не является простой технической неполадкой; сегодня они представляют угрозу, которая может иметь последствия для глобальной безопасности. Современные общества противостоят этим угрозам при помощи целого ряда действий и мер, которые все вместе называются кибербезопасностью.

Дальнейшие исследования должны быть направлены на поиск и использование рациональных и эффективных процедур для обеспечения динамичной (адаптируемой, осознанной, гибкой и продуктивной) жизнестойкости компьютерных сетей систем безопасности. Это позволит справляться с непредвиденными и непредсказуемыми событиями (неизвестными неизвестными) в результате действий как внутри организации, так и извне. В достижении этой цели ключевую роль будут играть люди и выполнение ими своих обязанностей на всех уровнях иерархии организации (кибербезопасность в сочетании с «человекоцентрической безопасностью»), что и должно стать основными объектами аналитической работы. □

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

СОЗДАВАЯ ПРОЧНУЮ БАЗУ ДЛЯ ЗАЩИТЫ ЖИЗНЕННО ВАЖНЫХ СЛУЖБ

Агниешка Вербитска, Департамент кибербезопасности, Министерство кибернетики Польши

За последние 10 лет информационные и коммуникационные технологии (ИКТ) стали жизненно важными для функционирования экономики и превратились в основную движущую силу развития во всех секторах. Правительства, бизнес-сообщество, общественные и частные организации и частные лица — все стали зависимы от цифровой среды в своей основной деятельности.

И по этой причине все они стоят перед лицом растущего количества неопределенностей. Угрозы безопасности кибернетическому, цифровому и аппаратному и программному обеспечению ИКТ возросли, увеличилось и количество нападений, что привело к серьезным негативным последствиям в таких сферах, как финансы, конфиденциальность и репутация, а в отдельных случаях был нанесен даже физический ущерб. Инциденты в области цифровой безопасности могут иметь далеко идущие экономические последствия для организаций. Примерами могут служить нарушение нормального функционирования (нападение типа «отказ в предоставлении услуг», нарушение гарантий конфиденциальности информации и саботаж), прямые финансовые убытки на сотни миллиардов евро, судебные иски, нанесение ущерба репутации, кражи интеллектуальной собственности, технологий и результатов исследований, потеря конкурентоспособности (кража торговых секретов), а также потеря доверия среди граждан, клиентов, сотрудников, акционеров и партнеров.

Мы часто слышим, что информация — это власть, а обмен информацией между партнерами — это ключевая ценность партнерства между общественным и частным секторами. Эта концепция особенно верна в мире, который двигается со скоростью света — со скоростью интернета. Своевременный, достоверный и оперативный обмен информацией, относящейся к кибербезопасности, между организациями — в критических секторах, между секторами, в пределах одной страны и в международных масштабах — является чрезвычайно важным для эффективного противостояния угрозам кибербезопасности организаций. Одним из наиболее важных результатов обмена информацией является установление доверия между людьми и организациями. Обмен информацией представляет собой эффективный метод управления совместными рисками в среде, где картина угроз постоянно меняется. Обмен информацией все больше поощряется законодателями и другими заинтересованными сторонами, которые осознают, что снижение рисков кибербезопасности для правительственных систем, критических объектов инфраструктуры и предприятий все в большей степени зависит от этой формы проактивного сотрудничества. Однако, выгоды в сфере безопасности, получаемые в результате обмена информацией, должны достигаться таким способом, чтобы при этом не наносился ущерб конфиденциальности и не ущемлялись права и свободы личности. Для того, чтобы программы обмена информацией широко использовались и были успешными, надежная защита конфиденциальности и гражданских свобод должна ставиться на первое место.

Ни одна организация не в состоянии справиться с полным спектром вопросов по обеспечению своей кибербезопасности и жизнестойкости своих компьютерных сетей в одиночку. Организации тяготеют к глобальной взаимосвязи и, соответственно, в одинаковой степени подвержены глобальным угрозам кибербезопасности. Поэтому, необходимо сотрудничество с партнерами с различной организационной, функциональной, секторальной и национальной принадлежностью и с

предприятиями, начиная от малых и средних и заканчивая многонациональными частными корпорациями и правительствами. Это чрезвычайно важно для противодействия динамичным и многоплановым угрозам для кибербезопасности, которые могут нанести вред организации и ее службам. Более того, критически важные объекты инфраструктуры в большинстве случаев находятся в частных руках. В частном секторе накоплен значительный опыт в развитии интернет-политики, создании компьютерных технологий и организации защиты против несанкционированного проникновения в сети.

Отношения партнерства используются организациями государственного и частного секторов для обмена информацией об инцидентах, уязвимых местах, угрозах, соответствующих стратегических вопросах, операционных методах и примерах наиболее эффективных решений. Ряд стран, таких как Германия, Голландия, Великобритания и США, приобрели значительный опыт посредством сотрудничества, при этом в ходе сотрудничества своими знаниями обменивались все заинтересованные стороны, такие как правительства, национальные агентства, регулирующие органы, компании, занимающиеся информационными технологиями (ИТ), фирмы по безопасности ИТ, крупные предприятия, частные объекты критически важной инфраструктуры и исследователи в области безопасности. Это сотрудничество развивалось неравномерно, в зависимости от ситуации, культурных особенностей и законодательных рамок в каждой конкретной стране. Некоторые из этих отношений между представителями государственного и частного секторов были закреплены законодательным или регулятивным образом. Другие создавались просто организациями-единомышленниками без всякого юридического оформления.

КЛЮЧ К УСПЕХУ

Создание обстановки доверия чрезвычайно важно для любого партнерства между общественными и частными организациями, поскольку информация, передающаяся в рамках такого сотрудничества, зачастую носит закрытый характер. Чрезвычайно важно создать атмосферу, в которой общественные и частные субъекты понимают требования друг друга к вопросам порядочности и действуют соответствующим образом. Доверие особенно важно тогда, когда сотрудничество базируется на добровольном обмене информацией и добровольном участии в партнерстве. В основанном на доверии партнерстве у всех его участников должно быть понимание того, что цель сотрудничества не в том, чтобы выявить у одного из партнеров слабое место или упущение в том, что касается кибербезопасности. Эффективно функционирующее партнерство создает атмосферу уверенности и доверия, что позволяет обмениваться примерами удачных и неудачных решений между заинтересованными сторонами, делиться опытом относительно предпринятых против них нападений, обсудить подготовительные меры или даже реагирование простых граждан и регулирующих органов на разнообразные аспекты такого широкомасштабного вопроса, как информационная безопасность. Доверие между участниками создается в зависимости от их вкладов, совместной деятельности и накопленного опыта.

Существуют различные методы построения доверия, такие как неформальные встречи, рабочие встречи малыми группами, прозрачность деятельности, телеконференции, сети доверия и репутация порядочного партнера. Центры обмена информацией и анализа или организации по обмену информацией и анализу, использование «Протокола светофора» и других стандартов устанавливают правила передачи информации. В рамках усилий по выработке доверия важно с самого начала создать отношения партнерства. Этого можно достичь, начав работать с партнером на ранних стадиях, в идеале вообще «с чистого листа», или привлекая партнеров из государственного или частного секторов на наиболее приоритетных этапах проекта или на этапах, когда надо достичь определенной цели.

Для углубления сотрудничества необходимо постоянное и регулярное взаимодействие между заинтересованными сторонами. Доверие также создается путем установления совместного руководства программами и механизма принятия решений, основанного на консенсусе партнеров. Эффективное партнерство между общественными и частными организациями характеризуется четким набором правил, регулирующих рамки сотрудничества, такими как меморандум о взаимопонимании, а в случае партнерства с большим количеством участников — соглашения об обмене (кибер) информацией (или, как минимум, разработка руководящих принципов и этикета, которые стороны будут соблюдать). Правила должны предотвращать конфликт интересов и исключать двусмысленность в отношениях, обозначать четкие сферы ответственности и отчетности, а также определять реально достижимые цели и установавливать стимулы для партнеров. Еще одним ключом к успеху является общий интерес, который создаёт основу для сотрудничества и ситуацию, при которой в выигрыше остаются все партнеры. Необходим баланс между частным сектором (который рассматривает угрозы для кибербезопасности с точки зрения возможных финансовых потерь и испорченной репутации) и общественным сектором (где кибербезопасность рассматривается как общественное благо).

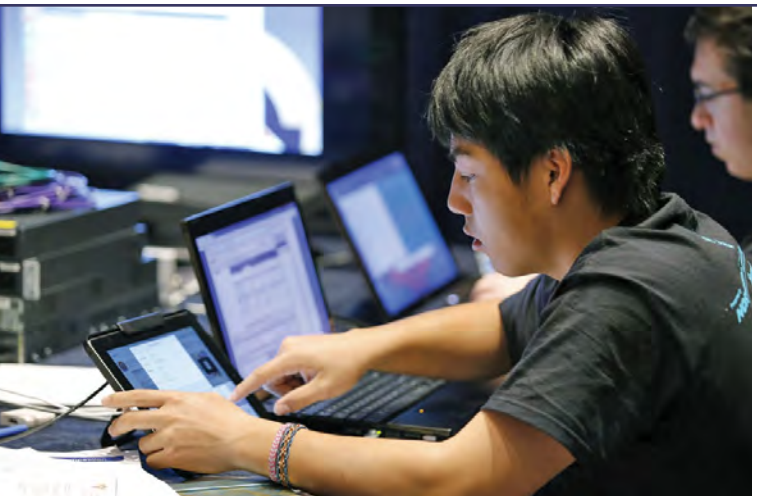
Для того, чтобы избежать недоразумений и ошибок, необходимо сразу внести ясность в такие аспекты, как возникновение напряженности или конкуренции. Если интересы партнеров не полностью совпадают, то тогда предлагается, чтобы их поведение регулировалось принятыми всеми сторонами правилами. Необходимо, чтобы

Министр иностранных дел Австралии Джули Бишоп, в центре, посещает центр операционной безопасности компании Telstra перед выступлением по случаю инаугурации «Стратегии международного киберсотрудничества» в Центре ознакомления посетителей компании Telstra в Сиднее в октябре 2017 г. EPA

каждая сторона имела четкое представление о приоритетах, целях и пределах возможностей своих партнеров. Это предотвращает возникновение конфликтных ситуаций из-за неправильной оценки партнера. Как государственные, так и частные организации должны иметь представление о движущих мотивах друг друга и быть в состоянии дать оценку, являются ли цели партнеров достаточно явными и совместимо ли функционирование такого партнерства с этими целями. Сотрудничество возможно только тогда, когда обе стороны понимают задачи и полномочия друг друга и стандартные операционные процедуры. Более того, топ-менеджеры организаций должны иметь четкое представление о целях и задачах и о том, как защита интересов акционеров способствует реализации целей и задач организации.

Обмен информацией в рамках партнерства приносит большие выгоды. Чрезвычайно важно, чтобы в течение определенного времени каждый партнер передал другим сторонам примерно такое же количество информации, какое он получил от других сторон. Это стимулирует каждого участника к сотрудничеству и повышает доверие в рамках партнерства. Второй, не менее важный плюс состоит в наработке сети надежных коллег. По мере того, как постепенно растет степень доверия, появляется желание и дальше продолжать обмен информацией. Энергичное участие каждой организации-партнера постоянно повышает ценность всех заинтересованных сторон вместе взятых, что служит движущей силой для продолжения партнерства. Приверженность партнерству на уровне топ-менеджеров государственных и частных организаций должна быть доведена до сведения всего персонала этих организаций.

Партнерские отношения складываются наилучшим образом, когда сотрудничающие организации находятся примерно на одном уровне зрелости. О степени зрелости



Олимпиада «Кибер-центурион», организованная совместно компанией Northrop Grumman, Национальной молодежной программой компьютерного образования «Американский кибер-патриот» и британской организацией Cyber Security Challenge, помогает в ликвидации пробелов в компьютерных знаниях. АССОШИЭЙТЕД ПРЕСС/GLOBE NEWSWIRE

организации свидетельствует ее желание обмениваться чувствительной информацией, относящейся к кибербезопасности, профессионализм и опыт персонала компании, отвечающего за кибербезопасность, и способность профессионально и безопасно обращаться с чувствительной информацией, полученной от других партнеров. Однако, в некоторых случаях уровень способности и зрелости партнерских организации различен. Более крупные организации еще могут получать выгоды от обмена информацией с меньшими по размеру организациями и от защиты таких организаций, поскольку это может позитивно сказаться на репутации всего сектора. У разных организаций разная история и разная модель функционирования, особенно у организаций из разных стран. У каждой из них своя культура, история, язык, правовая система, политические и этические предпочтения, а также свой опыт, процедуры, правила функционирования и практическая деятельность. Одни из них общественные организации, другие частные, и одни из них могут быть более открыты в сотрудничестве, чем другие.

Языковые барьеры могут возникать не только во время перевода с одного языка на другой, но и из-за разной лексики или технической терминологии (сленг, специфичный для конкретного сектора). Недостаточное внимание к этим различиям во время взаимодействия людей, технологий и процедур может негативно сказаться на сотрудничестве и обмене информацией. Помощь людей, способных преодолеть культурные барьеры, может способствовать беспрепятственному обмену информацией между разнородными партнерами. Более того, нельзя заставлять организации делиться информацией вопреки их воле. Если от них этого потребовать, то они могут продемонстрировать свое нежелание путем умышленного предоставления огромного количества ничего не значащей информации. Однако, в отдельных случаях, когда дело касается национальной безопасности или безопасности населения, сообщения об имевших место инцидентах с компьютерными сетями могут носить обязательный характер. В настоящее время идут дебаты между сторонниками принудительного и добровольного обмена информацией. Это не полный и окончательный список ключевых факторов, необходимых для установления и поддержания успешных партнерских отношений между общественными и частными организациями, но это те характеристики, которые были отмечены в ходе многочисленных исследований и которые стоит взять на заметку.

ПРОБЛЕМЫ

Партнерские отношения сталкиваются со многими проблемами, которые затрудняют обмен информацией. Иногда сообщения об обнаруженных уязвимых местах противоречат коммерческим интересам частных компаний, особенно, когда обнаружение и исправление недостатка прежде, чем о нем узнает конкурент, даст определенные рыночные преимущества. Общественный сектор также сталкивается с ограничениями при обмене информацией. Секретная и с ограниченным доступом информация, а также торговые секреты не могут передаваться людям, не имеющим необходимого допуска к секретным документам. Даже те сотрудники частного сектора, которые имеют допуск к секретным документам, зачастую ничего не могут делать с секретной информацией из-за существующих законов и правил. Более того, ожидания, что информация об угрозах, поступающая из государственного сектора в частный, окажется верной, приводит к длительному и тщательному процессу рассмотрения и пересмотра данных, что

задерживает выдачу критичной по времени информации. Высокая сменяемость кадров в государственном секторе часто негативно влияет на эффективность сотрудничества, особенно на аспект установления доверия. Нежелание делиться информацией может также происходить оттого, что пассивные партнеры или те, которые не делятся информацией, не несут никакого наказания или, потому что условия вступления в партнерство слишком облегченные и неформальные. Еще больший ущерб партнерству могут нанести недостаточное уважение к конфиденциальности информации или к установленным правилам сотрудничества, с которыми согласились все заинтересованные стороны. Продуктивный обмен информацией между организациями из разных стран также затрудняется разницей в законах и местных правилах, налагающих ограничения на обмен и хранение информации, а также правилами секретности и неразглашения информации.

Некоторые страны или отдельные сектора в экономике предполагают, что в соответствии с национальным или европейским законодательством обмен информацией об инцидентах с компьютерными сетями можно интерпретировать как поведение, нарушающее конкуренцию, и, потому, посягающее на существующие правила конкуренции. Более того, правоохранительные органы и другие общественные службы могут иметь задачи, вступающие в конфликт друг с другом, а их роль может иметь двусмысленный характер. Обмен детальной информацией об угрозах с целью повысить общее осознание сложившейся ситуации может также, при определенных юридических обстоятельствах, заставить правоохранителей предстать в новой роли и использовать эту информацию в целях проведения расследования. В результате источник информации может быть обнародован в суде, и может пострадать репутация организации, ставшей жертвой нападения. Национальные законы и правила в отношении защиты персональной информации выступают в качестве дополнительного барьера на пути процесса обмена информацией. Например, национальные законы, которые считают IP-адреса персональной информацией, не разрешают организациям обмениваться этой информацией, даже если это окажет помощь другим компаниям.

РЕКОМЕНДАЦИИ:

- **Обеспечьте участие всех слоев общества.** Партнерство должно использовать информацию, предоставляемую теми участниками, которые наилучшим образом подходят для достижения целей этого партнерства. Как общественные, так и частные субъекты имеют законные (хотя и разноплановые) интересы в сфере кибербезопасности и должны сотрудничать между собой. Поскольку залогом успеха является поддержка руководства на самом высоком уровне, участие в партнерстве государственного сектора должно включать представителей ключевых министерств, имеющих отношение к вопросам кибербезопасности. Участие государственных, местных и территориальных правительственных учреждений также является важным для обеспечения безопасности критической цифровой инфраструктуры на региональном и местном уровнях. Правительства разных стран также должны участвовать либо по межправительственным каналам, либо напрямую через партнерские отношения, чтобы обеспечить взаимодействие при решении как технических, так и политических вопросов. Наконец, для частного сектора сферой подходящего партнерства были бы как промышленные компании, так и некоммерческие организации; в число последних входят академические круги и защитники конфиденциальности и гражданских свобод. Например, привлечение некоммерческих организаций, занимающихся вопросами

Вице-президент Европейской Комиссии Андрус Ансип, слева направо, Комиссар Союза безопасности ЕС Джулиан Кинг и Комиссар Цифровой экономики и общества при ЕС Мария Габриэль выступают на тему кибербезопасности в Брюсселе. РЕЙТЕР

общественного управления посредством интернета, было бы необходимо для достижения координации политики, в то время как те организации, которые делают в своей работе упор на технологическом развитии, оказали бы большую помощь в продвижении исследований и разработок в сфере кибербезопасности. Представители академических кругов были бы также полезны в работе по обоим направлениям. Одинаково важным также является включение в число партнеров частного сектора промышленных компаний, от крупнейших корпораций до небольших стартапов. Более того, хотя поддержка на уровне высшего руководства в обоих секторах является залогом успеха, не менее важно иметь партнерские отношения и на тактических уровнях в организациях-партнерах для того, чтобы детальное обсуждение вопросов проходило между экспертами всех рангов.

- **Установите ясность относительно возможных напряженных ситуаций и конкуренции.** Похоже, что заинтересованные стороны в правительственных кругах считают кибербезопасность вопросом национальной безопасности. Они требуют, чтобы частный сектор приложил все знания и опыт для того, чтобы обезопасить киберпространство, и считают партнерские отношения общественным благом. В противоположность государственному сектору, частный сектор, похоже, считает кибербезопасность затратой, необходимой для охраны инвестиций в интеллектуальную собственность и в иные активы. Партнерство с общественным сектором представляет интерес только с той точки зрения, что оно служит цели увеличения прибыли. Четко установив конечную цель, партнеры легче смогут преодолеть культурные различия и достичь успеха, хотя достигать этого они будут совершенно разными путями.
- **Укрепляйте доверие, базирующееся на взаимной уверенности в том, что сотрудничество принесет выгоды обоим партнерам.** Доверие является ключевым элементом любых успешных отношений, оно достигается со временем и, как правило, через личные отношения. Партнерство между двумя секторами должно базироваться на правилах, способствующих долгосрочному сотрудничеству, поддерживаемому определенными стимулами. Правильно подобранный персонал — еще один путь к укреплению доверия. Участники партнерства, вносящие ценный вклад, который невозможно получить другим путем, будут укреплять стимулы к созданию доверительных отношений. Кроме того, отношения доверия должны быть взаимными. Это означает, что получатель информации не будет ею злоупотреблять и не нанесет вреда источнику, но, с другой стороны, будет доверять источнику настолько, чтобы быть уверенным, что информация подлинная и не вводит в заблуждение. Вот почему партнерства должны принять правила рассылки информации, такие как «Протокол светофора», чтобы дать источнику информации уверенность в том, что информация будет использована только так, как было ранее согласовано. Более того, в отдельных случаях необходимо заключить соглашение о неразглашении информации и достичь договоренности о правилах обмена чувствительной информацией.
- **Создайте стимулы для партнерства государственного сектора.** Хотя создание атмосферы доверия чрезвычайно важно для формирования настоящего партнерства, Рейчел Нисвандер Томас и Ларри Клинтон в своих трудах, опубликованных, соответственно, Центром стратегических и международных исследований и в журнале «Journal on Strategic Security», указывают, что также должны присутствовать стимулы, чтобы вознаградить каждый из секторов за сотрудничество. Когда мы говорим о подходе, основанном на побудительных мотивах, то лучше привязывать стимулирование к результату, чем к деятельности. Стимулы могут включать снижение уровня риска взлома системы путем создания более совершенной системы безопасности и жизнестойкости; экономию средств благодаря распределению труда при решении критической проблемы; доступ к конфиденциальной информации, получаемой от правительства; доступ к знаниям, которые невозможно получить никаким иным путем; возможность не соблюдать неадекватное предписание; возможность вносить вклад в стратегические решения и национальную политику; технические знания; развединформацию, исследования и анализ; подтягивание своих навыков, опыта и организационной структуры до уровня партнеров; и приостановление членства за отказ делиться информацией или пропуски совместных заседаний.
- **Установите правовые/регуляторные рамки.** Значительный рост партнерского сотрудничества в сфере кибербезопасности между государственными и частными организациями за последнее десятилетие позволяет сделать вывод, что общественные и частные субъекты могут работать вместе и без юридического оформления. Однако, правовые нормы могут помочь создать регулируемую среду, более благоприятную для добровольного партнерства в таких секторах как финансы или телекоммуникации. Если будет четкое разъяснение полномочий различных общественных институтов при оказании помощи частному сектору в случае незаконного проникновения в его сети, то это позволит общественным институтам более своевременно реагировать на запросы, что сделает их более привлекательными для партнерства в глазах частного сектора. Такие правила должны предотвратить появление конфликта интересов и снизить вероятность двусмысленных ситуаций.
- **Разработайте подход «снизу-вверх».** Партнерство,

Немецкий телекоммуникационный гигант Deutsche Telekom AG открыл крупнейший в Европе Операционный центр кибероборонs и безопасности в Бонне в октябре 2017 г. РЕЙТЕР

движимое в основном необходимостью обеспечения подконтрольности, будет требовать более жесткой инфраструктуры (и, возможно, сети отношений, основанных на какого-либо рода контракте), в то время как партнерство, ценящее гибкость, предпочтет более неформальные рамки. Учитывая, что кибербезопасность является аспектом национальной безопасности, может показаться логичным при формировании партнерства между частным и общественным секторами отдать предпочтение подконтрольности, а не гибкости. Однако, быстро развивающаяся природа киберугроз и необходимость в оперативном технологическом прогрессе для того, чтобы противостоять этим угрозам, делают гибкость чрезвычайно важным фактором в партнерствах по вопросам кибербезопасности. Это совсем не исключает возможность введения регуляторного механизма с целью поощрения подконтрольности, но структура самого партнерства в условиях эволюционирующего киберпространства должна быть достаточно гибкой, чтобы отвечать его целям.

- **Создайте крепкую и устойчивую финансовую базу (пример Великобритании).** Правительство может добавить такому партнерству ценность и снизить экономические барьеры, покрыв административные расходы и стоимость места проведения встреч.
- **Сделайте максимальной прозрачность.** Четко информируйте участников об актуальности и дополнительных преимуществах партнерства и будьте транспарентными в вопросах соблюдаемых правил и практических действий.
- **Правильно распределяйте и разделяйте риски.** Вопросы кибербезопасности должны быть частью непрерывного цикла управления рисками в организации.

ДВИГАЯСЬ ВПЕРЕД

Партнерство государственного и частного секторов остается чрезвычайно важным и эффективным инструментом для достижения целей кибербезопасности как в интересах государства, так и в интересах бизнес-сообщества. Совместные действия по предотвращению, защите, смягчению последствий и восстановлению после нападения является наилучшим способом обезопасить киберпространство. Но для смещения баланса в пользу жизнестойкости и прочной защиты, занимаясь одновременно и новаторскими разработками, требуется сосредоточение ресурсов на исследованиях и разработках, выработка соответствующей политики на национальном и международном уровнях и создание человеческого капитала в лице профессионалов высокого класса. Совместное создание экосистемы кибербезопасности способствует достижению целей как государства, так и бизнес-сообщества, поскольку обеспечивает развитие рынка и общественную безопасность. □

Высказанные в статье взгляды принадлежат только автору и не обязательно отображают официальную политику или позицию правительства Польши, Министерства кибернетики или любого другого правительственного учреждения.

СНИЖАЯ РИСКИ

ЧЕШСКАЯ РЕСПУБЛИКА ОТВЕЧАЕТ НА РАСТУЩИЕ УГРОЗЫ

Вероника Нетолицка
и Мартин Конечны

ФОТОГРАФИИ РЕЙТЕР

Нанесение ущерба критически важной информационной инфраструктуре (CII) Чешской Республики может негативно сказаться на национальной безопасности, поскольку под угрозой оказываются общие условия жизни населения, здравоохранение и экономика государства. Национальная стратегия кибербезопасности страны на период 2015-2020 гг., Ежегодный отчет Службы информационной безопасности за 2015 г. и Аудит национальной безопасности — все три документа признали существование серьезных угроз в этой области. Как свидетельствуют эти документы, кибершпионаж представляет серьезную угрозу CII. Однако, это не единственная угроза. Непроверенные и ненадежные поставщики аппаратного и программного обеспечения, засылки вирусов ради получения выкупа и кибертерроризм также представляют значительную опасность.

КИБЕРШПИОНАЖ

Кибершпионы стремятся получить ограниченного доступа стратегическую или важную информацию от отдельных лиц или организаций с использованием средств коммуникаций или при помощи нападения на них. Кибершпионы могут обеспечить политические, экономические или военные преимущества для вероятного противника, создавая значительную угрозу национальной безопасности.

Как указано в отчете Службы информационной безопасности Чешской Республики за 2015 г., основная опасность для страны в плане кибершпионажа исходит от России и Китая. В том году объектами российской кампании кибершпионажа стали два чешских министерства. Эти две страны занимались кибершпионажем и раньше, и их мишенями становились также и CII. В области CII, например, мишенью для нападения могут стать ведущиеся в Чешской Республике передовые исследования в сфере нанотехнологий, чем и известна страна. Соблазн получения исключительно важной информации технологического или политического характера делает эти исследования привлекательным объектом нападения.

Низкий риск обнаружения делает кибершпионаж особенно опасным. Во многих случаях идущая кампания шпионажа обнаруживается через месяцы, а то и годы после ее начала. Государства должны активно защищать себя от таких кампаний. Кроме того, полученная информация может использоваться не только в целях шпионажа, но иногда и в целях вымогательства или для дальнейшего распространения. Кибершпионаж также может функционировать в качестве основы для более изощренных кибернападений. Получение секретной информации может проходить посредством использования логина и персональных данных известных людей, которых впоследствии можно использовать в неблаговидных целях. По мере роста цифровых технологий и расширения CII количество и интенсивность кампаний кибершпионажа будет возрастать.

БЕЗОПАСНОСТЬ ЦЕПОЧКИ ПОСТАВОК

Как указывается в отчете Службы информационной безопасности за 2014 г., для создания угрозы для национальной безопасности может использоваться взлом системы безопасности цепочки поставок. Например, в компьютерные системы, обслуживающие CII, можно проникнуть, используя аппаратное обеспечение, в котором есть уязвимые места. В данном случае источник риска в полной зависимости государства от закупок аппаратного и программного обеспечения у внешних поставщиков, которые, в свою очередь, могут быть связаны с кибершпионажем.

Пример такого случая: в 2010 г. ВМФ США закупил у Китая тысячи микрочипов для широкого применения — от боевых ракет, ретрансляторов до пусковых установок гражданских ракет. Эти микрочипы, однако, имели «чёрный ход», позволяющий выключить всю систему, использующую эти чипы. В 2013 г. американский Конгресс официально охарактеризовал деятельность Китая как кибершпионаж. США запретили правительственные закупки у китайских компаний, а также рекомендовали, чтобы частные американские компании ограничили закупку программного обеспечения в Китае. Поскольку микрочипы могут быть запрограммированы таким образом, чтобы активно вмешиваться в работу системы, то важно проверять аппаратное и программное обеспечение, которое собираетесь использовать. В Чешской Республике, как и во многих других странах, подозрения падают на китайских поставщиков, таких как Huawei или ZTE.

ВИРУСЫ-ВЫМОГАТЕЛИ

Нанесение ущерба не ограничивается только аппаратным обеспечением. Могут также применяться злонамеренные программы, такие, как вирусы-вымогатели, которые блокируют компьютерные системы или шифруют записанную информацию и держат их в таком состоянии, пока не будет уплачен выкуп. Такие нападения также представляют значительную угрозу для CII.

Самые крупные вирусы этого типа (WannaCry, Petya), использовавшиеся для нападения на государственные инфраструктуры, напрямую не повлияли на Чешскую Республику. Однако, нет гарантий, что эта ситуация не изменится, поскольку такое криминальное использование вирусов очень прибыльное дело. Наилучшей защитой от заражения вирусом-вымогателем является, как минимум, копирование важных документов на носители, которые независимы от компьютеров, на которых хранятся данные. После нападения с применением такого типа вирусов, в большинстве случаев заблокированная информация не возвращается. Даже если она будет возвращена, после уплаты выкупа конфиденциальность уже нарушена.

КИБЕРТЕРРОРИЗМ

Кибертерроризм — явление относительно новое, и среди специалистов по безопасности нет единого мнения относительно его точного определения. Недавние нападения не подпадают под характеристики обычного терроризма. Согласно результатам Аудита национальной безопасности Чехии за 2015 г., кибертерроризм представляет меньшую угрозу для безопасности, чем кампании кибершпионажа. И хотя в настоящее время риск кибертерроризма не актуален для Чешской Республики, можно ожидать, что этот риск появится в будущем. Однако, обсуждение этого явления не стоит игнорировать, поскольку его потенциальные последствия для CII могут быть катастрофическими.

Фотографы работают на компьютерах в выборном штабе в Праге, Чехия, в 2017 г. Прочная законодательная база является ключевым фактором кибербезопасности.

ЗАКОНОДАТЕЛЬНЫЙ АСПЕКТ

Комплексная законодательная база представляет прочный фундамент для защиты CII. Закон о кибербезопасности, этот краеугольный камень законодательства в сфере кибернетики, вступил в силу 1 января 2015 г., спустя два года в него были внесены поправки.

Закон с внесенными в него поправками регулирует следующие сферы:

- Критически важную информационную инфраструктуру
- Операторов ключевых услуг (OES) (в соответствии с указанием службы сетевой и информационной безопасности (NIS))
- Важные информационные системы (IIS) общественных учреждений
- Провайдеров цифровых услуг (DSP) (в соответствии с указанием NIS)
- Провайдеров интернет-услуг (ISP)
- Крупные сети (или крупных ISP) с безопасными сетевыми соединениями за границей или с CII

Внедрение соответствующих подзаконных актов регулирует следующие аспекты:

- Требования к кибербезопасности
- Определяющие критерии OES
- Определяющие критерии IIS
- Безопасность правительственного «облака» (определение требований к безопасности для госучреждений)

Правительственным учреждением, отвечающим за кибербезопасность, является Национальное агентство компьютерной и информационной безопасности, при котором функционирует Национальный центр кибербезопасности (NCSC). NCSC имеет две составные части — Правительственную группу быстрого реагирования на компьютерные инциденты (CERT) и Отдел политики в сфере кибербезопасности. В соответствии с Законом о кибербезопасности, дополнительная CERT, отвечающая за кибербезопасность всей остальной страны — национальная CERT. Правительственная CERT защищает CII, OES и IIS и реагирует на инциденты в сфере

Оператор следит за демонстрацией протеста перед Пражским костелом в Чешской Республике в 2017 г. Нападения на информационные и коммуникационные системы угрожают национальной безопасности.

кибербезопасности; остальные регулируемые субъекты (ISP, крупные сети и DSP) находятся в ведении национальной CERT.

Еще одним законодательным актом, относящимся к CII, является Закон о кризисных ситуациях, который определяет процесс детерминации для элементов CII. Закон о кризисных ситуациях находится в компетенции Министерства внутренних дел. NCSC сотрудничает с Министерством внутренних дел по вопросам детерминации CII. Таким образом, роль NCSC, помимо помощи в реагировании на инциденты, заключается в том, чтобы оказывать поддержку в имплементации управления кибербезопасностью, проведении тестов на «пробиваемость» системы, проведении учений по кибербезопасности и оказывать поддержку в проведении образовательных мероприятий по тематике кибербезопасности.

NCSC также отвечает за проведение инспекций (аудиты уровня кибербезопасности) на всех участвующих объектах.

СНИЖАЯ РИСКИ

Принимая во внимание возможные последствия инцидентов в сфере кибербезопасности для национальной безопасности, защита CII и усилия OES являются первостепенными приоритетами для Чешской Республики. Соответственно, требования к контролю за кибербезопасностью на этой категории регулируемых предприятий отражают их важность.

Подход Чехии к снижению компьютерных рисков основан на оценке серьезности и характера рисков. Иными словами, подход основан на способности компаний/институтов справиться с потенциальными рисками, угрожающими их системам. Цель состоит в том, чтобы снизить риск нападений, которые могут привести к нежелательным последствиям, включая последствия на государственном уровне. CII и OES должны отвечать требованиям безопасности, определенным законом, чтобы снизить уровень риска. Эти требования описаны в Указе о требованиях к кибербезопасности и охватывают следующие технические области:

- Системы управления информационной безопасностью
- Управление активами и рисками
- Безопасность организации
- Политика безопасности и документация
- Управление цепочкой поставок
- Личная безопасность
- Управление операциями и коммуникациями
- Управление доступом к сетям
- Приобретение системы, ее развитие и обслуживание
- Обеспечение непрерывности обслуживания
- Физическая безопасность
- Безопасность сетей
- Безопасность персональной информации
- Защита от зловредных кодов
- Управление ведением документации
- Управление информацией относительно безопасности и инцидентов
- Безопасность компьютерных приложений
- Шифрование
- Промышленная кибербезопасность, управление функцией надзора и получения информации
- Безопасность цифровых служб
- Аудит

Проект измененной версии Указа о требованиях к кибербезопасности был составлен совместно с группой экспертов по кибербезопасности из частного и общественного секторов. Эта группа включала в себя представителей регулирующих организаций и экспертов в области кибербезопасности. Были включены рекомендации Европейского Союза и Агентства ЕС по сетевой и информационной безопасности.

Как уже упоминалось, NCSC обеспечивает поддержку практическому применению требований безопасности, обозначенных в этом указе. В 2017 г. NCSC начала проводить аудиты систем компьютерной безопасности наиболее важных правительственных организаций. Цель состоит в том, чтобы рекомендовать способы уменьшения риска, повысить кибербезопасность и усовершенствовать киберзащиту. Такие аудиты проводятся ежегодно.

ИЗВЛЕЧЕННЫЕ УРОКИ

Хотя законодательная база Чехии и принимаемые меры защиты создали прочный фундамент для защиты CII, кибербезопасность невозможно усовершенствовать без желания объектов CII защитить собственные системы. Таким образом, Чехия стремится создать особую среду, в которой операторы CII должны установить базовую защиту для укрепления безопасности своих систем.

Государство в этом играет важную роль, выступая больше как партнер, нежели как карающий орган. Начальным пунктом в этом процессе является налаживание отношений доверия между операторами CII и государством. Например, сейчас проводятся консультации между государственными экспертами и организациями CII относительно готовящихся законов. В 2017 г. был выбран нетрадиционный подход при выработке проекта Указа о требованиях к кибербезопасности, и до начала составления проекта могли высказать свои мнения и предложения профессионалы из различных слоев населения.

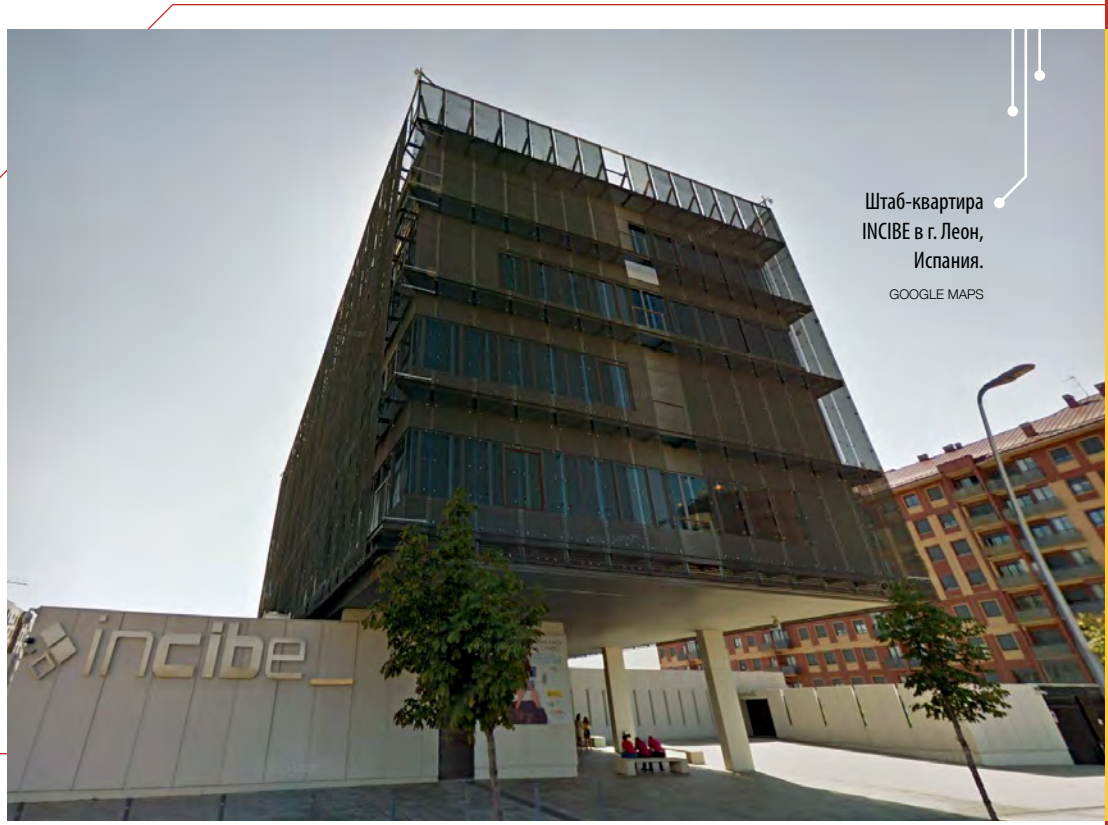
Подход, основанный на доверии, открывает возможности для обмена информацией. Эффективный обмен информацией позволит более глубоко понять надвигающиеся угрозы и внесет вклад в выработку соответствующих мер, внедрение которых может предотвратить компьютерные инциденты в будущем. Государства должны понять, что снижение рисков в киберпространстве — это бесконечный комплексный процесс, и государственные органы должны принимать в нем участие и занимать динамичную позицию во всех мероприятиях, относящихся к кибербезопасности. □

ЦИФРОВАЯ ОБОРОНА ИСПАНИИ

Применение новаторских моделей при защите критически важной инфраструктуры

Альберто Хернандес, Исполнительный директор,
Национальный институт кибербезопасности Испании (INCIBE)

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*



Штаб-квартира INCIBE в г. Леон, Испания.

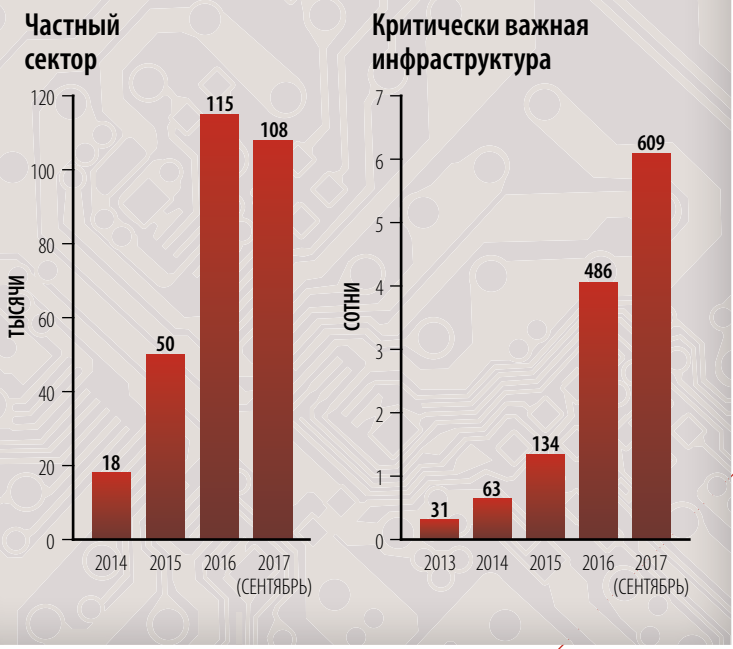
GOOGLE MAPS

За последнее время был совершен целый ряд крупномасштабных кибератак на критически важные службы и объекты инфраструктуры, которые широко освещались в средствах массовой информации. Но также были и нападения, которые нанесли такой же ущерб, но прошли в основном незамеченными. Количество таких нападений будет увеличиваться по мере того, как будет возрастать связь между индустриальными системами управления и расти количество коммуникационных сетей и приборов «интернета вещей». Такие возможности связи имеют много преимуществ в плане функционирования и управления, но порождают новые угрозы в сфере интернета и киберпространства. Глобальный масштаб киберпространства, низкая стоимость доступа к нему, анонимность, асимметричность и операционное время, измеряемое в миллисекундах — вот характеристики, которые способствуют быстрому развитию этих новых угроз.

Различные кибернападения наносят различный ущерб. В 2000 г. в Австралии в результате кибератаки, организованной недовольным сотрудником, в реки и парки г. Маручи вылилось более 2 млн. литров неочищенной воды. В 2008 г. в польском г. Лодзь четыре трамвая сошли с рельсов и несколько людей получили травмы после того, как 14-летний подросток переделал пульт дистанционного управления телевизором в прибор, способный переводить стрелки на трамвайных переездах. В 2010 г. был обнаружен Stuxnet. Это был первый известный вирус, созданный для шпионажа и перепрограммирования промышленных систем управления, отвечающих за критические объекты инфраструктуры, такие как ядерные электростанции. В более недавний период, в 2015 г., отключение подачи электроэнергии в сети оставило 1,5 млн. человек на несколько часов без электроэнергии в Украине. Эти кибернападения свидетельствуют о реальности угрозы нападения на ключевые службы и критические объекты инфраструктуры и о необходимости разработки и развития стратегии по снижению и управлению связанными с ними рисками.

В Испании количество инцидентов в сфере кибербезопасности, затрагивающих простых граждан и частный сектор, растет — с 18 тыс. в 2014 г. до 50 тыс. в 2015 г. и с более чем 115 тыс. в 2016 г. до 108 тыс. в период с января по сентябрь 2017 г. Что касается критически важных объектов инфраструктуры, то за последние четыре года количество инцидентов также возросло — с 31 в 2013 г. до 63 в 2014 г., 134 в 2015 г., 486 в 2016 г. и до 609 в период с января по сентябрь 2017 г. Реагирует на эти инциденты Группа безопасности и экстренного реагирования на компьютерные инциденты (CERTSI), управляемая Национальным институтом кибербезопасности Испании (INCIBE) и Национальным центром защиты критической инфраструктуры (CNPIC). Такой рост количества инцидентов в сфере кибербезопасности может быть вызван

ИНЦИДЕНТЫ С СИСТЕМАМИ КИБЕРБЕЗОПАСНОСТИ В ИСПАНИИ



Источник: CERTSI

тремя причинами: ростом числа кибернападений, повышением возможностей CERTSI по обнаружению инцидентов или повышенной степенью доверия между CERTSI и стратегическими операторами. Это свидетельствует о необходимости разработать стратегию защиты критической инфраструктуры, которая могла бы помочь организациям улучшить свою кибербезопасность.

Стратегия INCIBE

В 2007 г. Министерство внутренних дел Испании создало CNPIC с целью защиты национальных объектов критической инфраструктуры, в том числе и в киберсреде. С принятием в том же году закона о защите критически важной инфраструктуры Испания ввела в действие соответствующие стратегии и структуры для направления и координации действий различных общественных учреждений, занимающихся защитой критически важной инфраструктуры, при этом рассматривая кибербезопасность в качестве ключевого фактора во всех секторах.

Идет ремонт высоковольтных линий электропередачи возле г. Славянск, Украина. Кибератака на распределительную электросеть в 2015 г. оставила без электричества 1,5 млн. человек.

AFP/GETTY IMAGES

Для соблюдения регулирующих нормативов и реализации установленных практических мер по обеспечению кибербезопасности, INCIBE совместно с CNPIC разработал специальную целостную стратегию для критически важной инфраструктуры, охватывающую такие аспекты, как предотвращение кибератак, защиту от кибератак и реагирование в случае инцидента, угрожающего безопасности. Эта стратегия предусматривает следующие направления действий:

A. **ENSI:** Национальная система кибербезопасности известна как Национальная схема промышленной безопасности (ENSI). У нее есть общие методологии и инструменты для улучшения возможностей защиты, минимизации рисков, которым подвержены ключевые объекты; она также разрабатывает методологии и конкретные меры по снижению рисков, которые внедряются в промышленных организациях.

ENSI состоит из управления общей политики и трех подразделений, ответственных за следующие направления: меры по совершенствованию компьютерной жизнестойкости (IMC), модель развития возможностей кибербезопасности (C4V) и упрощенный механизм управления рисками в комплексной системе безопасности (ARLI-SI).

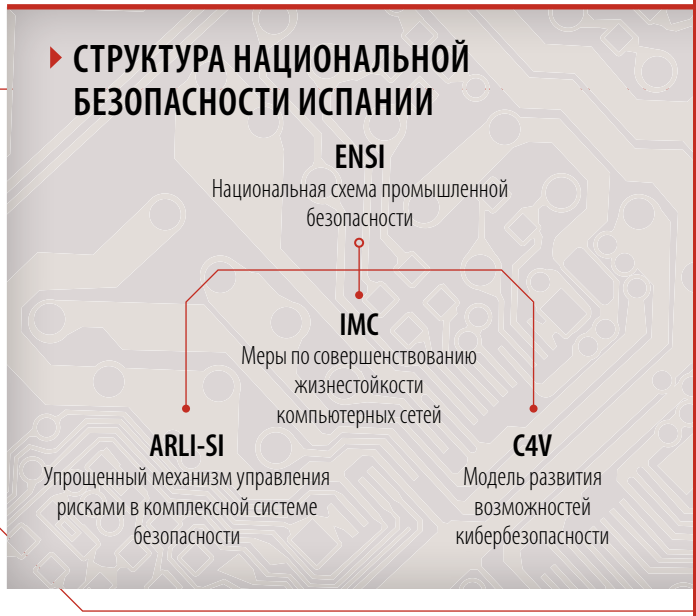
- **IMC:** Модель IMC определяет набор индикаторов повышения компьютерной жизнестойкости в качестве инструмента диагностики и измерения способностей противостоять катастрофам и неисправностям в цифровом пространстве и восстанавливанию после них.

Вопрос здесь не в том, станут ли организация и ее системы, включая ее компоненты, отвечающие за жизненно важные службы, объектами нападения, а в том, будут ли они должным образом подготовлены к противостоянию такому нападению, к тому, чтобы не допустить сбоев в работе ключевых служб и к восстановлению в самый короткий срок. Короче говоря, жизнестойка ли компьютерная сеть организации?

В компьютеризированном мире концепция жизнестойкости базируется на необходимости для организации быть в состоянии готовности быстро отреагировать на нападения, не допустить сбоев в предоставлении услуг, одновременно с этим совершенствуя свои возможности по идентификации, обнаружению, предотвращению и сдерживанию нападений, а также возможности восстановления после нападения и сотрудничества с партнерскими организациями.

INCIBE разработал эту комплексную структуру для измерения индикаторов компьютерной жизнестойкости организации после анализа Национальных стратегий кибербезопасности, в которых описаны основные стандарты, параметры и индикаторы, применимые в сфере безопасности.

СТРУКТУРА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИСПАНИИ



ЦЕЛИ IMC

Модель IMC включает 46 параметров, охватывающих четыре основные цели мер по обеспечению компьютерной жизнестойкости: предугадывать, противостоять, восстанавливаться и развиваться.

- **ARLI-SI:** Методология ARLI-SI — это упрощенная методология управления рисками, разработанная в качестве практичной и простой модели управления рисками. Ее основным компонентом являются промышленные системы управления, являющиеся отправной точкой и краеугольным камнем процесса совершенствования безопасности.

После стандартного аудита ключевых операторов предприятия знакомят с предварительным диагнозом состояния их систем безопасности. Однако, крайне необходимо также дать им дополнительную информацию о шагах, которые необходимо предпринять для улучшения системы безопасности, и о том, какой уровень кибербезопасности считается приемлемым.

- **C4V:** INCIBE разработал C4V, чтобы дать операторам понимание степени зрелости и надежности мер защиты, внедренных в системы критически важной инфраструктуры. В C4V обращено особое внимание на зависимость важных служб и на управление рисками в цепочке поставок информационных и коммуникационных технологий.

  Одно из преимуществ этой модели в том, что в случаях, когда сторонние провайдеры услуг оказывают влияние на уровень возможностей организации, то организация, несущая ответственность за услугу, должна сделать так, чтобы сторонние провайдеры также отвечали требованиям в отношении возможностей. Они также должны иметь процедуры мониторинга для того, чтобы этот уровень возможностей поддерживался постоянно на должном уровне на всем протяжении функционирования предприятия.

Б. Испанская платформа для обмена информацией об угрозах для кибербезопасности (ICARO) представляет собой инструмент, помогающий идентифицировать угрозы. Для предотвращения кибернападений и реагирования на них должным образом необходимо раннее оповещение. Для того, чтобы способствовать обмену информацией об угрозах и кибератаках, INCIBE разработал и внедрил ICARO, который работает на платформе обмена информацией о вирусах (MISP), использовавшейся для распространения индикаторов слабых мест, вызванных киберугрозами. При использовании ICARO, у критически важных операторов испанских предприятий появляется канал, который ускоряет процесс анонимизации обмениваемой информации и доступ к информации CERTSI. Эта платформа может также быть объединена с другими MISP по всему миру.

В. Национальная сеть промышленных лабораторий (RNLI) является платформой поиска информации о промышленных лабораториях с мощностями для экспериментальной работы и исследования решений по инфраструктуре на национальных промышленных предприятиях. RNLI преследует две цели: способствовать внедрению новаторских решений в промышленную кибербезопасность через сотрудничество и ускорение принятия решений, которые повышают конкурентоспособность местной промышленности.

Трамвай отъезжает с остановки в польском г. Лодзь. В результате кибератаки, устроенной подростком в 2008 г., четыре трамвая сошли с рельсов.
AFP/GETTY IMAGES

ДЛЯ ПРЕДОТВРАЩЕНИЯ КИБЕРНАПАДЕНИЙ И РЕАГИРОВАНИЯ НА НИХ ДОЛЖНЫМ ОБРАЗОМ НЕОБХОДИМО РАННЕЕ ОПОВЕЩЕНИЕ.

INCIBE выступает одним из организаторов ежегодного конкурса CyberEx, на котором рассматриваются различные сценарии тестирования жизнестойкости компьютерных сетей.

INCIBE

RNLI позволяет операторам находить информацию о национальных инфраструктурах и создавать точку пересечения между спросом и предложением по вопросам кибербезопасности. Другие преимущества включают продвижение взаимодействия и сотрудничества между всеми вовлеченными сторонами и ускорение обмена экспертными знаниями в среде специалистов.

Г. INCIBE взаимодействует с производителями, компаниями, специализирующимися в кибербезопасности, лабораториями и операторами объектов критической инфраструктуры с целью разработки новых инструментов улучшения кибербезопасности на критически важных объектах и для совершенствования возможностей обнаружения CERTSI.

При помощи этих инструментов INCIBE и CERTSI могут предоставлять новые услуги, например, подавать сигналы тревоги операторам с уязвимыми приборами промышленного управления. Когда INCIBE получает сигнал тревоги от производителя относительно конкретного прибора, INCIBE находит операторов, у которых имеется такой прибор, и посылает им оповещение со всей информацией, необходимой для самозащиты.

Другие дополнительные инструменты обеспечивают проактивное обнаружение систем промышленного управления, доступных через интернет, позволяя INCIBE улучшить свою систему оповещения.

Д. В качестве последнего элемента общей стратегии, национальные учения по кибербезопасности в Испании позволяют протестировать и усовершенствовать возможности кибербезопасности операторов критически важных объектов. В рамках этой инициативы под названием National CyberEx было проведено уже несколько учений. В 2015 г. учения были сосредоточены на банковском секторе, а в 2016 г. они были разработаны таким образом, чтобы провести оценку и повысить устойчивость к атакам сразу нескольких секторов, давая участникам учений ощутимые выгоды.

В ходе этих учений, в которых в командах операторов участвуют представители всех соответствующих специальностей, участники совершенствуют свои возможности ответных мер и повышают координацию между организациями.

Выводы

Глобальный масштаб и природа проблем кибербезопасности при защите объектов критической инфраструктуры требуют комплексного подхода, при котором необходимо предпринять целый ряд действий. Эти действия связаны с такими аспектами, как передовые технологии и их производители, существующая нормативная база, пользователи и человеческий фактор. Также крайне необходимы эффективная координация между всеми заинтересованными сторонами и постоянная приверженность новаторскому подходу и движению вперед. □

ПЕРЕЗАГРУЗКА БЕЗОПАСНОСТИ

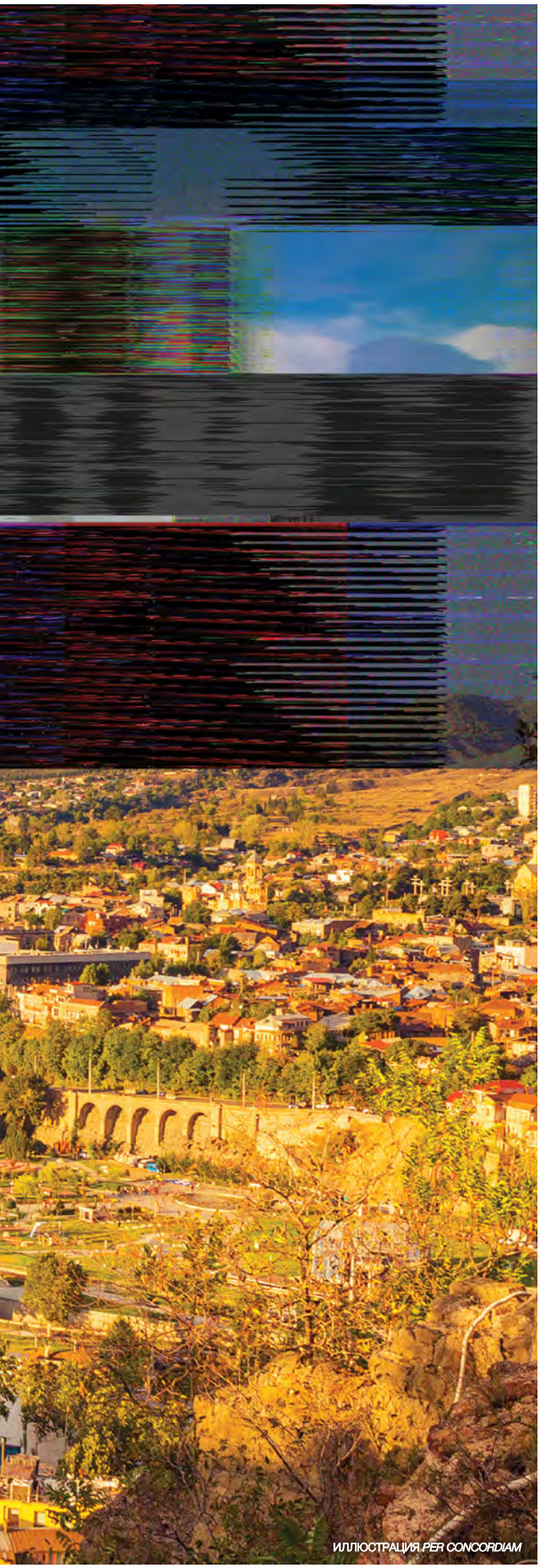


ИЛЛЮСТРАЦИЯ PER CONCORDIAM

Новаторский план защиты критической инфраструктуры Грузии

Андрия Готсиридзе и Мака Петриашвили

В XXI веке киберпространство, наряду с воздухом, землей, морем и космосом, стало пятой сферой, где происходят конфликты. Страны все больше эксплуатируют киберпространство ради достижения политических или военных целей или получения геополитических преимуществ. Число государств, успешно создающих наступательные кибервозможности, постоянно растет, а кибервойна быстро становится составной частью войны и конфликта.

Россия, в частности, успешно интегрировала элементы кибернападений в свою тактику гибридной войны. Ее наступательные действия в киберпространстве охватывают военные, дипломатические, политические, экономические, социальные, культурные и религиозные аспекты, которые она использует для нанесения ударов с техническими и психологическими последствиями. В результате опыта, приобретенного в ходе кибернападений и информационных операций в Эстонии (2007 г.) и Грузии (2008 г.), Россия усовершенствовала свою тактику кибернападений и теперь применяет ее в Украине. Анализ этих нападений доказывает, что Россия использует конфликтные территории в качестве полигона для тестирования своих возможностей кибернападений.

Транспарант на центральной площади в Тбилиси, Грузия, в августе 2008 г. после вторжения российских войск в страну. РЕЙТЕР

Кибератака против Эстонии в 2007 г. была предпринята с целью спровоцировать общественное недовольство. Это была первая признанная попытка использовать кибернападение для влияние на политические процессы. Уже в следующем году во время российско-грузинской войны российская киберстратегия переросла в хорошо организованные нападения, которые были синхронизированы с военными операциями и нацелены на создание информационного вакуума, распространение дезинформации и блокирование каналов международной поддержки правительства Грузии.

Российский опыт кибератак получил дальнейшее развитие во время нынешнего конфликта в Украине. Еще во время предыдущих операций в Эстонии и Грузии Россия продемонстрировала возможности использовать крупных операторов сотовой связи для ведения разведки и наблюдения, что позволяет определить местонахождение пользователя и получить информацию. Эти возможности широко использовались для сбора информации, оказания психологического влияния и определения и передачи координат для артиллерийских обстрелов. Впервые Россия напала на энергетические системы Украины и отключила их. За последние два года Россия расширила круг своих кибератак за пределы бывших советских республик, и хакеры, связанные с различными российскими правительственными структурами, вмешиваются в выборные процессы в Европейском Союзе и Соединенных Штатах.

СЕРЬЕЗНЫЕ УГРОЗЫ

Российские компьютерщики представляют серьезную угрозу для Грузии. Они несут ответственность за наступательные кибероперации, включая пропагандистскую деятельность, внедрение вирусов в промышленные системы управления (ICS) противника и проведение специализированных операций в компьютерных сетях и кибердеятельность в интересах других подразделений вооруженных сил России.

Одновременно с этим Россия создает инструменты для удаленного доступа к критической инфраструктуре ICS. Анонимные хакеры уже смогли получить доступ и нарушить работу программного обеспечения ICS крупных компаний, занеся в них вирус.

После российских кибератак на энергетическую систему Украины можно предположить, что в будущих конфликтах российские нападения не ограничатся атаками «отказ в обслуживании» (DDoS-атаками), удалением информации и кибершпионажем. Нет никакой гарантии в том, что нападающие не выберут своими объектами критически важную инфраструктуру, что может привести к масштабным разрушениям и человеческим жертвам, хотя даже относительно простые нападения типа DDoS-атак или стирания информации могут нанести слишком большой вред плохо защищенной инфраструктуре.

Наряду с причинением сбоев и ущерба компьютерным сетям, Россия прибегает к разрушительным кибердействиям психологического характера с целью оказания влияния на поведение и взгляды оппонента. Для военных приоритетом является развитие информационных возможностей на периоды войны, мира или кризисных ситуаций для того, чтобы контролировать информационный контент и механизмы распространения информации.

Масштабы киберугроз, стоящих перед Грузией, возрастают, поскольку угрозы становятся все более сложными и разнообразными, а кибернападения, организованные или поддерживаемые Россией, могут

В Таллине, Эстония, прошли учения по киберзащите «Сомкнутые щиты – 2017», организованные Центром совместной киберзащиты НАТО. Для Грузии важно участвовать в международных киберучениях. РЕЙТЕР

Президент Украины Петр Порошенко выступает в Тбилиси, Грузия, в 2017 г. Порошенко, который приблизил свою страну к Западу, несколько раз был объектом нападения хакеров. АССОШИЭЙТЕД ПРЕСС

привести к значительным материальным потерям и человеческим жертвам. Киберпропаганда может негативно повлиять на общественное мнение и взгляды населения Грузии по отношению к Западу. При этом будет формироваться и укрепляться имидж пророссийской элиты и провоцироваться ситуация, которая может подтолкнуть Россию к проведению военных операций. Таким образом, Грузия должна уделять особое внимание созданию и внедрению механизмов сбора и анализа информации, чтобы лучше оценивать намерения, возможности и действия России, являющейся опасной кибердержавой.

СИЛЫ КИБЕРРЕЗЕРВА

Для Грузии необходимо интегрировать кибервозможности и защиту компьютерных сетей в военные операции. Страна просто обязана ввести в состав своих Вооруженных Сил квалифицированных специалистов в области кибернетики. Недостаток компьютерных знаний, особенно знаний в сфере киберзащиты, является проблемой государственного сектора в целом. Даже в развитых странах, где государственная служба дает более значительные материальные выгоды, чем в Грузии с ее ограниченным бюджетом, интеллектуальный потенциал в области информационных технологий сосредоточен в бизнес-секторе. Поскольку кибербезопасность является коллективной ответственностью, а критически важная инфраструктура в основном принадлежит частному сектору, для противостояния кризисным ситуациям в военное и мирное время необходимо тесное сотрудничество между частным и государственным секторами, некая модель партнерства государственных и частных структур. Более того, когда главная угроза исходит от такого государства, как Россия, которая широко использует доморощенных хакеров с вымышленными именами типа КиберБеркут, Тролли из Ольгино, а также интернетботы, то сотрудничество частного и государственного секторов просто необходимо.

В свете этих угроз со стороны России создание «киберрезерва» — системы добровольной мобилизации специалистов по информационным и компьютерным технологиям — является целенаправленным решением. Такой киберрезерв даст возможность государству мобилизовывать по всей стране человеческие киберресурсы на время войны или кризисных ситуаций. Киберрезервисты будут использовать свои знания и опыт в случае чрезвычайных ситуаций. Эта система также принесет пользу и бизнес-сектору, поскольку специалисты по информационным технологиям будут иметь возможность участвовать в различных обучающих программах и учениях, которые обычно доступны только государственным служащим. Такой набор специальных знаний очень важен для эффективного управления кризисными ситуациями, например, такими, какие имели место после использования вирусов WannaCry и Petya. В качестве примера наиболее эффективных решений можно привести Литву и Австрию, где специалистов по информационным технологиям призывают в силы резерва, и Эстонию, где успешно создана практически на добровольной основе «Лига обороны».

Киберрезервисты будут набираться на добровольной основе. Киберрезерв будет состоять из специалистов по информационным технологиям из банков, интернет-провайдеров, компаний-операторов мобильной связи, энергетических компаний и других технологических компаний. Эти резервисты будут нести службу на добровольной основе и призываться через Национальную гвардию Грузии. Все добровольцы должны будут пройти сертификацию о получении должного образования в области информационных технологий и иметь соответствующие навыки и знания, чтобы отвечать установленным для резервистов квалификационным требованиям.

Их подготовка будет охватывать общие принципы информационной безопасности и специализированные вопросы кибербезопасности. Вместе с тем, резервистов обучат базовым навыкам кибервойны и информационных операций. Служба в киберрезерве будет альтернативой прохождению обязательной военной службы.

Выгоды для государства:

- Улучшенные возможности кибероборонны, отвечающие уровню современных проблем и угроз.
- Вооруженные Силы получат дополнительные возможности проведения компьютерных и информационных операций.
- Киберзащита, укрепленная за счет привлечения высококвалифицированных профессионалов в области информационных технологий при минимальном использовании людских ресурсов и финансовых затрат.

Выгоды для киберрезервистов:

- Возможность пройти специальное обучение, которое финансируется государством и которое недоступно для обычного населения.
- Возможность проходить службу в резерве в

Банкомат в Украине отключен от интернета в результате волны кибернападений на украинские организации в 2017 г. Украина испытывает массированные кибератаки со стороны России. EPA

качестве альтернативы обязательной военной службы.
- Поддержание и совершенствование профессиональных навыков, находясь в резерве.
- Служба в качестве специалиста в случае войны или кризисной ситуации.

Выгоды для бизнес-сектора:
- Повышение квалификации сотрудника за счет программы обучения, финансируемой государством.
- Инфраструктура компании будет иметь более совершенную защиту.
- Работники — резервисты не будут в обязательном порядке призываться в армию.
- Развитие методологии киберзащиты применительно к работе частного сектора.

Ожидаемые результаты:
- Создание дополнительных возможностей в плане информационных и компьютерных операций в вооруженных силах.
- Улучшение сотрудничества и координации между государственным и частным секторами.
- Внедрение киберэлементов в военные операции.
- Интеграция прошедших отбор специалистов в национальную оборону при минимальных затратах.

РАНЕНЫЕ ВОЕННОСЛУЖАЩИЕ

Кроме того, программа киберрезерва даст возможность реинтегрировать раненых военнослужащих в национальную оборону. В Грузии примерно 1 500 военнослужащих, получивших ранения в российско-грузинской войне 2008 г. и в международных миротворческих операциях в Афганистане и Ираке, которые не могут проходить действительную службу по состоянию здоровья. Однако, после прохождения подготовки их можно будет включить в киберрезерв.

Основные причины включения раненых бойцов в киберрезерв следующие:
- У раненых грузинских бойцов высокий уровень патриотизма и желания служить своей стране.
- Став киберзащитниками, они смогут полноценно реинтегрироваться в общество.
- Их знакомство с военной тактикой и стратегией и понимание реального боя соотносятся с реалиями боев в киберпространстве.

Какие выгоды получат наши раненые военнослужащие?
- Останутся на военной службе.
- Внесут вклад в совершенствование национальных возможностей киберзащиты.
- Получат самые современные навыки в новейшей и одной из важнейших сфер безопасности.
- Продолжат вести активный образ жизни.
- Получат компенсацию за заслуги перед родиной.

ЗАКЛЮЧЕНИЕ

Киберпространство является ключевым элементом в гибридной тактике, и в сегодняшнем мире оно используется все чаще и чаще, в том числе и в Грузии. И поэтому необходимо на постоянной основе включить киберкомпонент в военные учения на национальном уровне и обеспечить участие государственных и частных учреждений Грузии в международных киберучениях. Эффективная киберзащита требует тесного сотрудничества между государственными учреждениями и частными компаниями.

Проект киберрезерва можно и нужно начать для оказания мощной поддержки этому сотрудничеству и для создания национальных кибервозможностей. Интеграция специалистов по информационным технологиям из частного сектора в механизм защиты критически важной инфраструктуры даст Грузии адекватные возможности ответа на разрушительные кибернападения со стороны сильного агрессора. □

AFP/GETTY IMAGES

БЕСПОКОЙСТВО СЕГОДНЯШНЕГО ДНЯ

В СВЯЗИ С БЫСТРЫМ РОСТОМ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА КОСОВО ДОЛЖНО УКРЕПИТЬ СВОЮ ЗАЩИТУ

Хафизе Байрами
начальник отдела ИТ, Силы безопасности Косово

Сегодня интернет является частью профессиональной и личной жизни многих миллионов людей по всему миру. Быстрое развитие технологий делает обеспечение кибербезопасности серьезной проблемой. Многие услуги в государственных и общественных секторах предоставляются через интернет, где пользователям угрожают вирусы, вредоносные коды, кибершпионаж и фишинг.

Дым поднимается из труб угольной электростанции в г. Обилич, неподалеку от Приштины, Косово. РЕЙТЕР

В Косово наблюдается резкий рост числа пользователей интернета, и в настоящее время произошел прорыв в охвате рынка, подобный тому, который был в европейских странах. Киберпреступления были определены в качестве одной из глобальных угроз, которая может вызвать ухудшение уровня безопасности Косово, и озабоченность на этот счет уже была высказана в правительственном докладе «Анализ обзора сектора стратегической безопасности Республики Косово» за 2014 г. На основании этого Косово стало создавать более развитые возможности киберзащиты. Так же, как и во многих других странах, наиболее важными сферами, нуждающимися в защите, являются критически важная инфраструктура (CI) и критически важная информационная инфраструктура (CII).

Защита включает такие элементы, как законодательная база, стратегия и правила и определение круга заинтересованных лиц и механизмов, отвечающих за различные аспекты CI и CII. Поскольку киберугрозы присутствуют практически везде, необходимо, чтобы Косово пересмотрело свои приоритеты в плане инвестиций, уделяя особое внимание безопасности и гармонизации законодательной базы, которая бы регулировала такие вопросы, как инциденты с безопасностью компьютерных сетей и защита информации. Законодательные базы должны быть гармонизированы на национальном и международном уровнях, поскольку киберпреступления не имеют таких обычных ограничений, как границы, гражданство, пол или возраст.

Все правительственные структуры должны составить исчерпывающий список всей CII. В Косово такого полного списка CII нет. В 2016 г. был составлен проект закона о защите CI. Положения этого проекта закона полностью копируют Директиву Совета ЕС 2008/114/EC об идентификации и назначении всей европейской CI и о шагах, необходимых для улучшения их защиты.

В соответствии с этим законом, идентификация и приоритизация национальных CI должна возглавляться Министерством внутренних дел и осуществляться по согласованию с органами безопасности, государством, правительственными и неправительственными организациями, владельцами и операторами государственных и частных объектов, а также с основными международными заинтересованными лицами. Чрезвычайно важно идентифицировать и провести оценку реально существующих CII внутри страны и принять все необходимые меры для их защиты.

ЗАКОНОДАТЕЛЬНАЯ БАЗА

В начале 2016 г. Ассамблея Косово одобрила Национальную стратегию кибербезопасности и План действий для реализации этой стратегии. В Косово также приняты законы, регулирующие многие вопросы, относящиеся к кибербезопасности, включая предотвращение киберпреступлений и борьбу с ними, услуги информационного сообщества и правительственных учреждений, электронные средства коммуникации и защиту персональных данных.

Базовые законодательные положения, относящиеся к киберпреступлениям и киберинцидентам, приведены в Уголовном кодексе и в Уголовно-процессуальном кодексе. Есть также Закон об Агентстве по чрезвычайным ситуациям, регулирующий сотрудничество и взаимодействие правительственных органов, на основе которого и составляются планы реагирования на чрезвычайные ситуации. Органы безопасности реагируют на кризисную ситуацию в соответствии с планами реагирования, в которых больше внимания уделяется природным катастрофам и другим кризисным ситуациям, чем киберинцидентам. Для того, чтобы ввести в этот план инциденты в сфере кибербезопасности, власти Косово должны обновить его или составить новый, более эффективный план. У каждой организации есть соответствующие административные инструкции и стандартные операционные процедуры или руководящие указания, призванные защищать информационные сети.

ЗАИНТЕРЕСОВАННЫЕ ЛИЦА И МЕХАНИЗМЫ

В соответствии с национальной стратегией, в 2016 г. в качестве высшего руководящего органа по вопросам кибербезопасности был создан Национальный совет по кибербезопасности. Этот совет возглавляет заместитель министра внутренних дел, и в его работе участвуют следующие министерства и ведомства: Министерство внутренних дел; полиция Косово; Агентство судебной экспертизы; Министерство сил безопасности Косово; Разведывательное управление Косово; Агентство информационного сообщества; Совет безопасности Косово; Министерство юстиции; Прокурорский совет Косово; Судейский совет Косово; Министерство финансов; Таможенное управление Косово; Министерство образования, науки и технологий; Министерство иностранных дел; Регулирующее управление электронной и почтовой связи (RAEPC); и Центральный банк Косово.

Национальная группа реагирования на чрезвычайные компьютерные ситуации (CERT) была создана и подчинена RAEPC. Она стремится достичь необходимых возможностей в плане людских и технических ресурсов, инфраструктуры и услуг. Другие правительственные учреждения также создают CERT-ы для своих нужд.

ОБРАЗОВАНИЕ, ОБУЧЕНИЕ И ПРОВЕДЕНИЕ УЧЕНИЙ

Государственному и частному секторам трудно справляться с проблемами, возникающими в связи с быстрым технологическим развитием и новыми услугами информационных технологий. Министерство образования выделило в качестве приоритетных направлений коммуникации и технологии. Свидетельством такой приоритизации может служить тот факт, что в учебных планах на всех образовательных уровнях упор делается на информационные и коммуникационные технологии (ICT) и вопросы безопасности. Предпринимаются усилия по созданию программ кибербезопасности для начальных и средних школ.

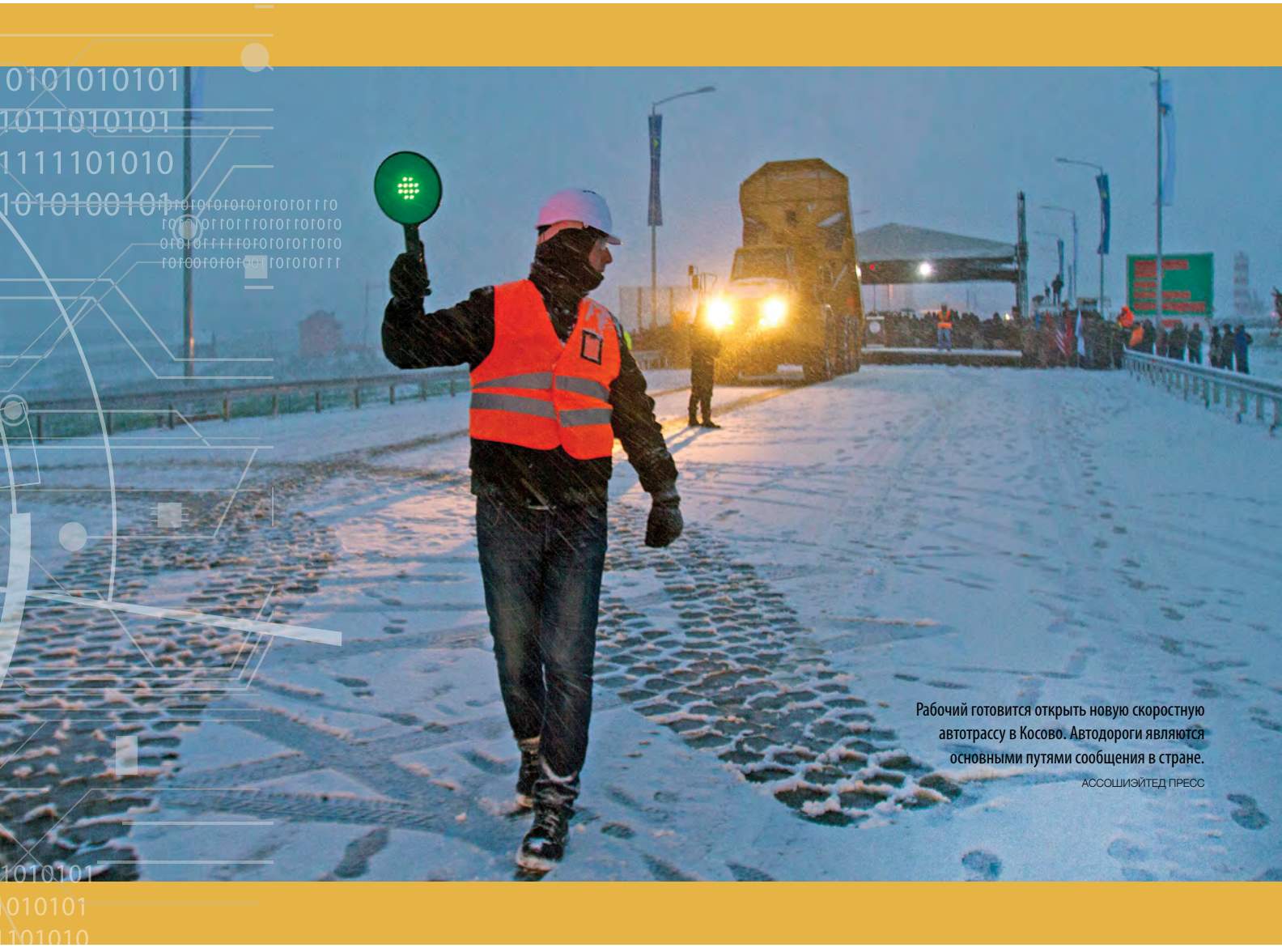
Для правительственных пользователей ICT Институт общественного управления Косово ввел правила обучения, разработанные Министерством общественного управления. Это министерство ежегодно проводит обучение для пользователей по вопросам безопасности информации в соответствии с различными запросами от отдельных министерств и других правительственных организаций.

Важной частью правительственной координации и взаимодействия является составление сценариев и проведение по ним совместных учений, в ходе которых участвующие организации могут проверить свои возможности реагирования на современные вызовы. Эти учения повышают возможности реагирования на различные угрозы как на национальном уровне, так и на уровне отдельного министерства или ведомства. После одобрения стратегии национальной безопасности каждое ведомство провело киберучения для повышения осознания проблемы среди пользователей; также были запланированы учения для проверки готовности к межведомственному сотрудничеству.

РЕКОМЕНДАЦИИ

Понимание следующих моментов улучшит ситуацию с кибербезопасностью в стране:

- При составлении национальной стратегии кибербезопасности за основу были взяты руководящие принципы Агентства Европейского Союза по безопасности сетей и информации (ENISA). Для того, чтобы лучше синхронизировать стратегию, технологическое развитие и международное законодательство и привести законодательство Косово в соответствие с законодательством таких международных организаций, как ЕС, НАТО, ООН и другие, еще предстоит принять другие законы.
- Все организации, ответственные за кибербезопасность, должны разработать и гармонизировать правила и процедуры по защите критически важной информации и инфраструктуры. Эти правила должны неукоснительно соблюдаться, с тем, чтобы обеспечить взаимодействие между организациями как внутри Косово, так и за его пределами.
- Необходимы более масштабные инвестиции в национальную CERT, с тем, чтобы сделать ее полностью функциональной, укомплектовать соответствующим персоналом, оснастить оборудованием и инструментарием, провести необходимое обучение, что, в свою очередь, откроет дорогу к аккредитации в организации «Надежный разработчик» (Trusted Introducer) и в глобальном Форуме групп безопасности и реагирования на инциденты (FIRST). «Надежный разработчик» — это организация, созданная сообществом европейских CERT для того, чтобы решать общие проблемы и оказывать поддержку всем группам реагирования на чрезвычайные компьютерные ситуации.
- Национальная CERT должна иметь полномочия налаживать сотрудничество с региональными и международными организациями CERT.
- Необходимо провести тщательную работу по идентификации всех CII и принять меры для их защиты.
- Нужно способствовать сотрудничеству и обмену информацией между ключевыми организациями государственного и частного секторов посредством эффективного сотрудничества.
- Будет полезно организовывать и участвовать в международных мероприятиях по вопросам кибербезопасности, таких как конференции, семинары и «круглые столы». Не менее полезными будут ролевые игры и учения по кибербезопасности с участием всех заинтересованных организаций с целью проверить уровень межведомственного взаимодействия.
- Необходимо разработать учебные планы для гражданских учебных заведений, чтобы знакомить пользователей интернета с вопросами защиты информации и конфиденциальности. Особый упор при этом надо делать на защиту детей от отдельных материалов, появляющихся в интернете, для чего необходимо создавать программы для родителей, разъясняющие все риски выхода детей в интернет.
- Нужно организовывать образовательные кампании и обновить нынешние учебные планы ICT в средних учебных заведениях и ввести в них курсы по кибербезопасности. Указ ENISA о безопасности сетей и информации и Инициатива образовательных мероприятий по вопросам кибербезопасности, с которой выступил американский Национальный институт стандартов и технологий, могут служить примерами программ по повышению информированности общества в вопросах кибербезопасности.
- В государственных учреждениях и частных компаниях, имеющих дело с информационными и



Рабочий готовится открыть новую скоростную автотрассу в Косово. Автодороги являются основными путями сообщения в стране.

АССОШИЭЙТЕД ПРЕСС

коммуникационными технологиями, важно обучать и сертифицировать сотрудников, отвечающих за информационную безопасность.

ЗАКЛЮЧЕНИЕ

Киберпреступления продолжают представлять наиболее серьезную угрозу учреждениям в Косово. Страна приняла конкретные меры для создания законодательной базы, нацеленной на предотвращение и борьбу с любого рода киберпреступлениями. Однако, остаются нерешенными еще много проблем, особенно в том, что касается технических возможностей противостоять кибератакам. Это — относительно новая сфера деятельности для Косово.

Существует постоянная необходимость в укреплении базы организаций, отвечающих за предотвращение киберпреступлений и наказание за них. В этих организациях необходимо модернизировать технологическое оборудование, поддерживать международное сотрудничество в области обмена информацией, а также дать полномочия тем органам, которые лучше всего могут справиться с киберугрозами. Также необходимо улучшить координацию между правоохранительными органами и техническим персоналом, чтобы лучше разбираться во всех сложностях киберпреступлений.

И, наконец, необходим устойчивый механизм повышения образовательного уровня и информированности населения в вопросах кибербезопасности и проведение киберучений для определения и устранения недостатков, которые имеются в Косово в плане безопасности коммуникационной и информационной инфраструктуры. Введение учебных планов с курсами по кибербезопасности во всех учебных заведениях, начиная с начальных школ, создаст в Косово среду, способствующую созданию возможностей по борьбе с киберугрозами и осознанию рисков, которые эти угрозы представляют, что поможет развитию в стране прочной структуры кибербезопасности. □

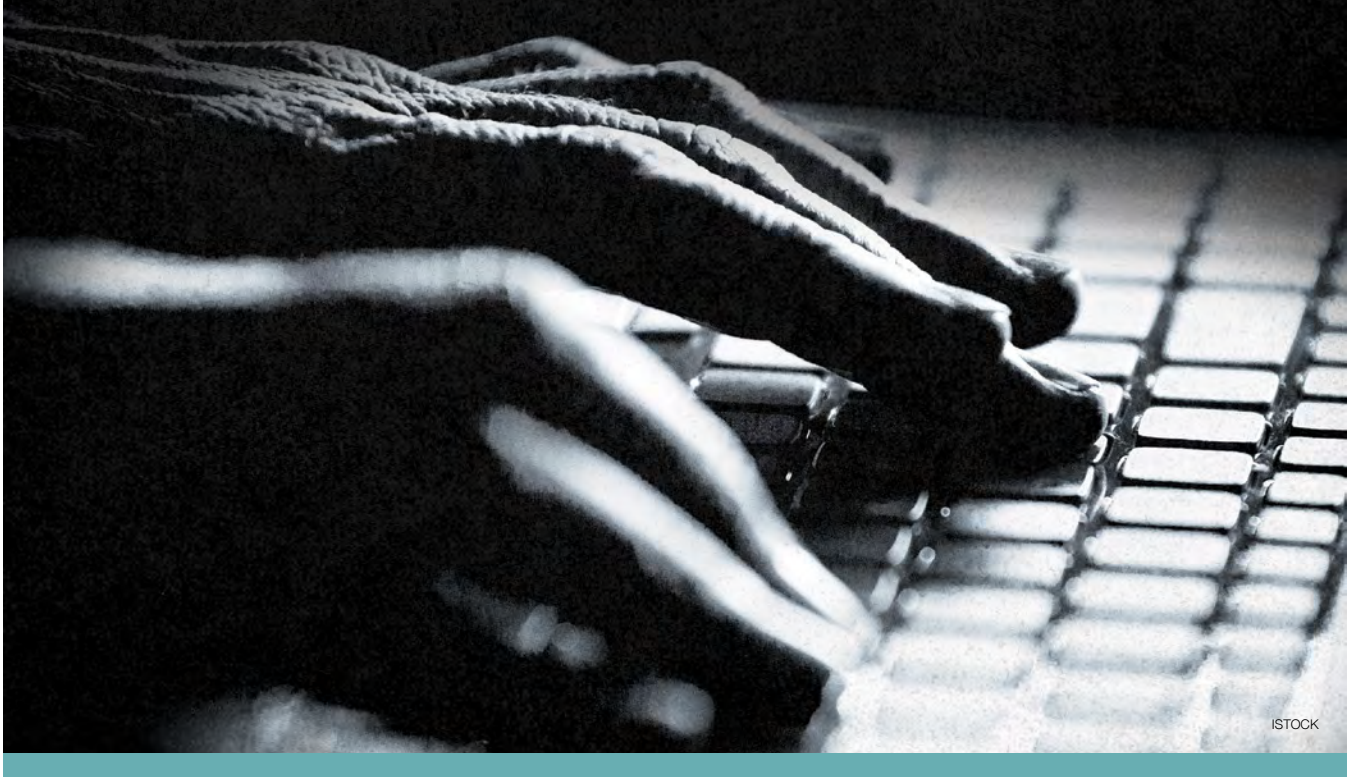
КОВАРНЫЕ УГРОЗЫ

ДЛЯ ЗАЩИТЫ КИБЕРПРОСТРАНСТВА ТРЕБУЕТСЯ СТРАТЕГИЧЕСКОЕ ПРЕДВИДЕНИЕ

Майор Волбери Ногуейра де Лима Сильва, Вооруженные Силы Бразилии

В историческом плане внедрение новых технологий привело к трем важным промышленным революциям. Первая революция произошла в результате изобретения паровых машин; использование электричества привело ко второй промышленной революции; третью революцию вызвало изобретение компьютеров, приведшее к автоматизации производственных процессов.

Нынешний тренд — «Индустрия 4.0», использующий технологии, относящиеся к кибер-физическим системам, «интернету вещей» и хранению информации в «облаке». Благодаря этим новшествам сегодня возможно создавать «разумные фабрики», объединяющие человеческие способности принимать решения с компьютеризированной автоматизацией, делая производственный процесс более рациональным и эффективным.



ISTOCK

Характеристики «Индустрии 4.0» включают взаимодействие между механизмами и людьми; прозрачность информации; техническую помощь, позволяющую системам поддерживать человеческую способность принимать решения и выполнять опасные работы; и децентрализованное, автономное принятие решений по специфическим работам с использованием кибернетических инструментов.

ЭВОЛЮЦИЯ ВОЙНЫ

Внезапность — один из основных принципов войны и совместных операций. Исторические примеры свидетельствуют о том, что применение стратегии «противовеса» для создания преимущества довольно часто приводило к быстрой победе над противником. Первый такой «противовес» (ядерное оружие) и второй «противовес» (стелс-технологии и управляемые боеприпасы) использовались Соединенными Штатами и НАТО для противостояния стратегическим преимуществам Советского Союза и Варшавского Договора во времена «холодной войны».

По мнению Министерства обороны США, третий «противовес» основывается на технологиях и концепциях следующего поколения и направлен на обеспечение стратегического превосходства над противниками, используя, например, достижения в области искусственного интеллекта и автономность, интегрированную в систему боевых действий. Современная война очень сложна и требует эффективного командования и управления военными силами с использованием быстрого и децентрализованного процесса принятия решений. Информация об обстановке на поле боя поступает благодаря C4ISR (командование, управление, коммуникации, компьютеры, разведка, наблюдение и рекогносцировка). Технологии третьего «противовеса» позволяют это сделать.

Киберпространство — одна из пяти взаимозависимых сфер наряду с воздухом, землей, морем и космосом,

Пятый форум бразильской Группы реагирования на инциденты в сфере компьютерной безопасности, проведенный в сентябре 2017 г. в Сан-Паулу, собрал вместе экспертов из частного сектора, академических кругов и правительственных структур для обмена информацией и уроками, извлеченными во время Олимпийских Игр в Рио-де-Жанейро в 2016 г. ВООРУЖЕННЫЕ СИЛЫ БРАЗИЛИИ

но в современной войне эта пятая сфера накладывается на остальные четыре. В нашем спорном и беспорядочном мире объединенные силы требуют наличия повышенных кибервозможностей, которые переведут наиболее важные сражения в «виртуальный театр боевых действий», ставя целью уничтожение сетей и цифровых систем противника.

ГЛОБАЛЬНЫЕ УГРОЗЫ

В глобализованном мире информационного века существует тенденция к интеграции всех стран в единое киберпространство без каких-либо границ. Информационные и коммуникационные технологии (ICT) все больше входят в жизнь общества — в государственную сферу, в частный сектор и в личную жизнь людей. При помощи ICT правительства, население и многонациональные корпорации связывают свои системы по всему миру во взаимозависимую сеть, которая зависит от нескольких физических и виртуальных узловых центров, имеющих уязвимые места и подверженных воздействию кибертерроризма и преступности, шпионажу и хакерским атакам. На это указывает Агентство Европейского Союза по безопасности сетей и информации.

Киберпространство служит опорой современному обществу и обеспечивает важную поддержку мировой экономике, но при этом оно само имеет множество серьезных потенциально уязвимых мест, которые могут не только подорвать чью-то личную конфиденциальность, но и сорвать работу критически важной инфраструктуры, нанеся ущерб городам, штатам и даже всей стране.

В настоящее время на планете 3,6 млрд. людей, связанных между собой интернетом; при этом также растет количество пользователей «интернета вещей». Это одно из наиболее уязвимых мест для кибератак, поскольку многие простые пользователи не знают, как правильно установить и использовать средства безопасности на своих подсоединенных устройствах, открывая тем самым двери для киберпреступников. Из-за большого количества слабых мест преступный вход в сети обходится недорого, он может иметь место абсолютно везде и при этом обладает относительной анонимностью. Об этом пишет Фил Уильямс в своей книге «Киберпространство: злонамеренные субъекты, криминальные возможности и стратегическое соревнование». Нападающие могут действовать в одиночку против одной выбранной цели или же организовываться в преступные

группировки для нападения на сложные системы, используя, например, изощренные настойчивые угрозы.

В соответствии с Военной доктриной кибероборонны Бразилии, критически важная инфраструктура состоит из объектов, услуг, товаров и систем, нарушение работы или разрушение которых может привести к серьезным последствиям для правительства, социального и экономического секторов, а также и к возможным международным последствиям. В зависимости от степени серьезности нападения, использованного слабого места и ущерба, причиненного любому из этих секторов, национальная безопасность и экономика страны могут сильно пострадать. Именно поэтому так важно сотрудничество между всеми партнерами по киберзащите.

На эту тему можно привести несколько последних примеров. В 2007 г. серия нападений на многочисленные веб-сайты в Эстонии, включая веб-сайты банков, национальных министерств, газет и службы телерадиовещания, нанесла серьезный ущерб стране.

Отсутствие системы обеспечения кибербезопасности и соответствующих правил увеличивает уровень угрозы (кто нападает), уязвимость (слабое место, которое атакуется) и последствия (ущерб от нападения). По этим причинам необходимы объединенные международные меры с задействованием комплексного подхода к усилению мер киберзащиты в рамках соответствующего мирового законодательства.

СТРАТЕГИЧЕСКОЕ ПРЕДВИДЕНИЕ

Серьезное отношению к решению такой огромной проблемы, как защита киберпространства, требует точного понимания оперативной обстановки. Среди имеющихся в наличии различных инструментов, метод стратегического предвидения представляет собой хороший способ увидеть всю картину целиком посредством моделирования, например, моделей, построенных с помощью таких методов, как анализ силового поля, метод графической визуализации возможных прямых и непрямых последствий под названием «колеса будущего» и просчет возможных результатов действий.

А. Анализ силового поля: он графически изображает взаимоотношения между различными силами, участвующими субъектами, интересами и т.д., задействованными в конкретной проблеме, и интенсивность этих взаимоотношений. Например, рис. 1 приводит к выводу, что киберугрозы носят глобальный характер.

Б. «Колеса будущего»: эта диаграмма выделяет тенденции и показывает потенциальные последствия, когда на киберпространство влияют различные факторы (см. рис. 2).

В. Просчет возможных результатов действий: этот подход позволяет выявить благоприятные и неблагоприятные условия, а также вероятность того, что эти условия наступят (см. рис. 3).

ЗАКЛЮЧЕНИЕ

У киберпространства нет границ или пределов, и преступники, хакеры, воинствующие экстремистские организации и злонамеренные субъекты могут повысить нестабильность в мире, причинив ущерб гражданским и военным организациям в любой точке мира. Компьютерная среда служит основой современного общества, обеспечивая очень важную поддержку мировой экономике, гражданской инфраструктуре, общественной и национальной безопасности.

Мировые угрозы в киберпространстве Анализ силового поля *Рис.* 1

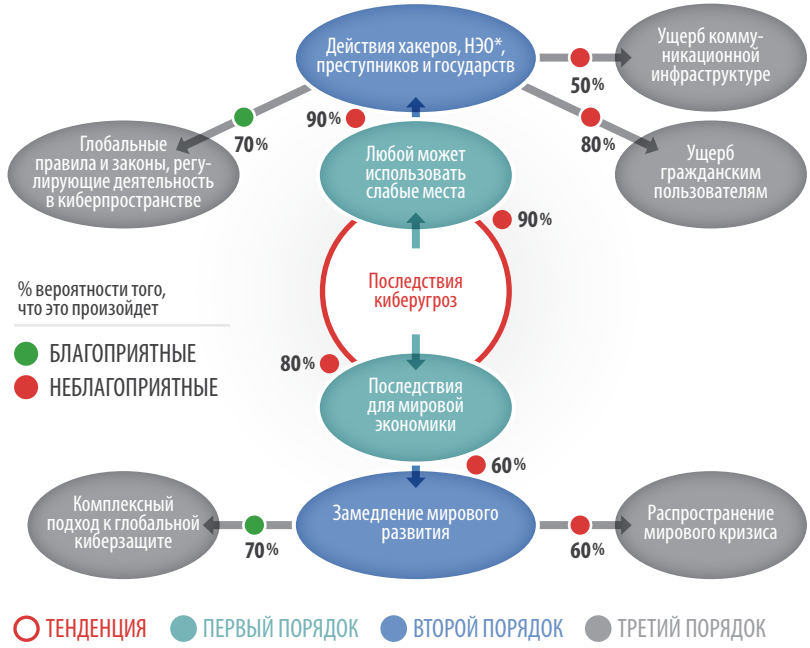
Источник: майор Волбери Ногуейра де Лима е Сильва

«Колеса будущего» *Рис.* 2

*Насильственные экстремистские организации

Источник: майор Волбери Ногуейра де Лима е Сильва

Просчет возможных результатов действий *Рис.* 3



Насильственные экстремистские организации

Источник: майор Волбери Ногуейра де Лима е Сильва

Эта проблема вызывает тревогу. Для решения этой проблемы требуются долгосрочные и постоянные усилия, основанные на единстве и сотрудничестве между странами, международными организациями, неправительственными организациями и частным сектором, применяя при этом всеправительственный подход.

Для того, чтобы избежать неблагоприятных условий, обозначенных в методе просчета возможных результатов действий, необходимо предпринять следующие шаги:

- Наладить обмен информацией через единую систему, чтобы снижать и ликвидировать киберугрозы.
- Практиковать коллективный подход и обмен информацией о наиболее эффективных вариантах решения проблем.
- Повысить информированность общества относительно масштаба проблем кибербезопасности.
- Дать критический анализ аспектов кибербезопасности, таких как стратегия, политика, законодательная база и международное сотрудничество.
- Ввести в сферу кибербезопасности всеправительственный подход.
- Повысить сотрудничество между государственным и частным секторами.
- Расширить масштабы исследований на тему информационной безопасности и привлечь к ним международные академические круги.
- Обеспечить проактивную координационную поддержку со стороны международного сообщества.

Ради сохранения свободы волеизъявления и собраний, уважения к собственности, к правам на интеллектуальную собственность и конфиденциальность и ради предотвращения самовольного и незаконного нарушения этих прав, необходимо международное сотрудничество в сфере кибербезопасности.

И, наконец, основной ценностью, которая позволяет налаживать долгосрочное и эффективное сотрудничество между различными заинтересованными лицами в кибернетической сфере, является доверие. □

ВЗЛАМЫВАЯ КОМПЬЮТЕРНЫЕ СЕТИ ПЕНТАГОНА

РЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ И ДРУЗЬЯ-СЫЩИКИ ПЕНТАГОНА ПОМОГАЮТ УКРЕПИТЬ БЕЗОПАСНОСТЬ

Материал редакции *per Concordiam*

ФОТОГРАФИИ ПОЛКОВНИКА ЛИРНЕСТА РУФФИНА/ВВС США

Для обороны любого государства чрезвычайна важна защита от кибернападений. По мере того, как тактика противника развивается, и новые технологические усовершенствования противника открывают новые уязвимые места в вашей системе защиты, основным требованием является внедрение новых технологий. Вот почему Министерство обороны (МО) США начало программу «Взломай Пентагон», смелую инициативу, направленную на совершенствование киберзащиты.

Эта программа, начатая в 2016 г., была первой инициативой такого рода в федеральном правительстве США. Она дает возможность частным лицам участвовать в поиске программных ошибок и уязвимых мест в вебсайтах МО, которые доступны широкой публике.

«Мы знаем, что поддерживаемые государством специалисты и «хакеры — чёрные шляпы» хотят добраться до наших сетей, — сказал бывший министр обороны Эш Картер во время открытия программы. — Но чего мы полностью не понимали до того, как запустили эту пилотную программу, так это то, как много есть «хакеров — белые шляпы», которые хотели бы улучшить ситуацию, помочь сделать так, чтобы наш народ и наша страна были в большей безопасности».

Примерно 14 тыс. т.н. «хакеров» зарегистрировались для участия в этой программе, которая координируется группой киберобслуживания МО. Они согласились следовать установленным правилам, а взамен им выплачивали определенную сумму, если они действительно находили уязвимое место в компьютерных платформах МО. В качестве объектов для «взлома» были выбраны следующие вебсайты: Defense.gov, DoDlive.mil, DVIDSHUB.net и MyAFN.net.

«Когда мы говорим об информации и технологиях, оборонный истэблишмент, как правило, делает ставку на закрытые системы, — пояснил Картер. — Но чем больше дружелюбно настроенных глаз смотрят на наши системы и вебсайты, чем больше недостатков мы сможем найти и чем больше уязвимых мест мы сможем исправить, тем более высокий уровень безопасности мы сможем предоставить нашим военным на поле боя».

Первое уязвимое место было обнаружено уже через 13 минут после того, как была запущена эта пилотная программа, а всего в течение первых шести часов было подано 200 сообщений об обнаруженных недостатках. За месяц за найденные недостатки было выплачено в общей сложности 75 тыс. долл США.

Один из хакеров — школьник-старшеклассник — сказал, что он благодарен за такую предоставленную уникальную возможность. «Это была отличная практика — считает Дэвид Дворкен. — Я начал все чаще участвовать в этих программах «Нашел баг — получи деньги», и считаю их полезными — как в плане денег, так и потому, что ты делаешь что-то нужное, чтобы защитить информацию в режиме онлайн».

Считается, что программа прошла с большим успехом. Были обнаружены сотни уязвимых мест, пропущенных программистами МО, включая больше десятка таких, которые относились к группе высокой степени риска. Об этом сообщила Кейт Шарлот, ведущий директор по вопросам киберполитики в канцелярии министра обороны США. Она рассказала об этой программе специалистам — компьютерщикам из стран Ближнего Востока во время конференции по вопросам коммуникаций в странах Центрального региона (CRCC), организованной Центральным командованием США (CENTCOM) в апреле 2017 г. в г. Александрия, штат Вирджиния, США. Сухопутные силы США также планируют провести аналогичную программу.

Кроме этого, МО разработало процедуру оповещения о замеченных слабых местах на любом из сайтов МО, открытых для публичного пользования. Так же, как и программа «Нашел баг — получи деньги», эта процедура первая в федеральном правительстве США. По сути, она напоминает более широкую программу борьбы с преступностью и терроризмом под названием «Увидел что-то подозрительное — сообщи», но с особым упором на кибербезопасность.

Количество уязвимых мест растет

Необходимость в таких программах растет в геометрической прогрессии. Детские игрушки, холодильники, домашние системы безопасности и светофоры — вот только несколько предметов из огромного списка устройств из нашей повседневной жизни, которые включаются от интернет-сигнала. Каждый новый предмет представляет своего рода компромисс — в то время как он приносит людям по всему миру удобство и новшество, этот, основанный на интернет-технологиях предмет, может стать объектом хакерской атаки. Система кондиционирования воздуха в комнатах, где хранятся

Член Совета директоров Администрации регулирования коммуникационных и информационных технологий Кувейта Мухаммад Алтура делает презентацию о достижениях своей страны в обеспечении кибербезопасности на конференции в 2017 г.

Директор Департамента систем командования, управления, коммуникаций и компьютерных сетей генерал-лейтенант Сухопутных войск США Митчел Килго беседует со своим коллегой из Саудовской Аравии генерал-лейтенантом Рийад бин Абдул Азиз Аль-Дугейтер в перерыве между сессиями проходившей в 2017 г. конференции по проблемам кибербезопасности.

правительственные компьютерные серверы, может подвергнуться атаке и остановить работу, что приведет к сбоям в работе компьютерных сетей. Кукла, которая записывает голоса, чтобы развлекать и успокаивать детей, может также записывать и приватные разговоры, которые ведутся в доме. По мере развития технологий растет также и число потенциальных слабых мест, что делает готовность противостоять взлому компьютерной сети как никогда важной.

Для решения этих проблем представляется совершенно необходимым создание возможностей для военных, академических кругов и экспертов из государственного и промышленного секторов наладить сотрудничество и пересмотреть роль каждого в обеспечении национальной безопасности. CRCC была одной из таких возможностей; ее основное внимание было сосредоточено на ответных мерах в случае инцидента с компьютерными сетями. Установленные в ходе конференции

10 ВЕДУЩИХ СТРАН В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Мировой индекс кибербезопасности (GCI) за 2017 г. показывает, что приверженность идее кибербезопасности не зависит от географического региона. Три из десяти стран, входящих в десятку стран с самым высоким уровнем кибербезопасности, находятся в азиатско-тихоокеанском регионе, две находятся в Европе, а две в Северной Америке. Оставшиеся три страны находятся в Африке, на Аравийском полуострове и на Кавказе.

СТРАНЫ РАСПОЛОЖЕНЫ В СПИСКЕ В ЗАВИСИМОСТИ ОТ ИХ ПРОГРЕССА В ПЯТИ КЛЮЧЕВЫХ ОБЛАСТЯХ.

1. **Законодательство:** наличие правовых учреждений и законодательной базы в сфере кибербезопасности.
2. **Техническая сторона:** наличие технических организаций и структур, занимающихся кибербезопасностью.
3. **Организационный аспект:** наличие институтов, координирующих политику и вырабатывающих стратегию на национальном уровне.
4. **Наращивание возможностей:** наличие исследовательских, образовательных и обучающих программ; сертифицированных профессионалов и государственных учреждений, стимулирующих наращивание возможностей.
5. **Сотрудничество:** наличие партнерских отношений, договоренностей о сотрудничестве и обмен информацией с коллегами.

отношения между специалистами помогают организациям восстановиться после нападения быстрее и с меньшими потерями.

«Я считаю, что самая лучшая оборона — это проявление инициативы первым», — делится своим мнением во время конференции заместитель командующего CENTCOM генерал-полковник Чарльз Браун-младший. Он пояснил, что любая страна становится сильнее в результате сотрудничества различных организаций внутри страны и с киберэкспертами в других странах мира.

Для достижения такого сотрудничества необходимо отказаться от культуры «информационных башен», которая существует во многих организациях. Это поможет руководителям принимать решения на основе всей имеющейся информации, объясняет директор Департамента систем командования, управления, коммуникаций и компьютерных сетей генерал-лейтенант Сухопутных войск США Митчел Килго. «Вы должны хорошо знать свою критически важную инфраструктуру и ее слабые места, — подчеркивает Килго. — Вы должны представлять, с какими рисками может столкнуться задание и с какими рисками может столкнуться критически важная инфраструктура. Командирам это необходимо знать».

На конференции с докладами выступили представители частных компаний и академических кругов. Иностранные высокопоставленные госчиновники давали примеры наиболее эффективных решений применительно к своим странам, высказывая свое мнение по тематикам, заслуживающим дальнейшего обсуждения.

«В Ираке рост популярности интернета — для использования в целях безопасности, для профессиональной деятельности и в личных целях — совпал с отсутствием безопасной киберинфраструктуры, — пояснил ситуацию директор Управления военных коммуникаций Министерства обороны Ирака генерал-лейтенант Махди Ясир Зубаиди. — Это повышает необходимость понимания опасности киберпреступлений, сопровождающих почти каждую технологическую разработку, особенно в контексте превращения общества в своего рода киберсообщество».

По мнению экспертов, для того, чтобы создать надежную киберзащиту, одного программного обеспечения мало. Для того, чтобы лучше защитить компьютерные сети и обнаружить уязвимые места, системные администраторы должны пройти специальную подготовку и уметь представить себе образ мышления противника и знать способы «охоты» на него в сетях.

Отдельные страны, такие как Кувейт, смогли успешно внедрить всеправительственный подход к вопросам кибербезопасности. Член Совета директоров Администрации регулирования коммуникационных и информационных технологий Кувейта Мухаммад Алтура представил детальный доклад о процессе развития стратегии в своей стране. Кувейт определил цели, на которых необходимо сосредоточить внимание в следующие три года. Были приняты три основные стратегические инициативы: развивать в Кувейте культуру кибербезопасности; защищать и постоянно поддерживать безопасность национальных активов, включая критически важную инфраструктуру, информационные и коммуникационные технологии, а также интернет; и развивать сотрудничество, координацию и обмен информацией с партнерами по вопросам кибербезопасности как внутри страны, так и за рубежом.

«На сегодняшний день отсутствует международное законодательство в сфере кибербезопасности, — указал Алтура. — Что касается военных, то законодательство в отношении защиты суверенитета страны очень четкое. А в области киберзащиты такого законодательства нет». □

В этой статье использовалась информация, предоставленная Министерством обороны США и фирмой HackerOne, занимающейся проблемами кибербезопасности.

	Страна	Балл GCI	Законодательство	Техническая сторона	Организационный аспект	Наращивание возможностей	Сотрудничество
1	Сингапур	0.92	0.95	0.96	0.88	0.97	0.87
2	США	0.91	1	0.96	0.92	1	0.73
3	Малайзия	0.89	0.87	0.96	0.77	1	0.87
4	Оман	0.87	0.98	0.82	0.85	0.95	0.75
5	Эстония	0.84	0.99	0.82	0.85	0.94	0.64
6	Маврикий	0.82	0.85	0.96	0.74	0.91	0.70
7	Австралия	0.82	0.94	0.96	0.86	0.94	0.44
8	Грузия	0.81	0.91	0.77	0.82	0.90	0.70
9	Франция	0.81	0.94	0.96	0.60	1	0.61
10	Канада	0.81	0.94	0.93	0.71	0.82	0.70

ИСТОЧНИК: МЕЖДУНАРОДНЫЙ СОЮЗ ТЕЛЕКОММУНИКАЦИЙ

Система баллов: 1 – наивысший балл

ВМЕСТЕ МЫ СИЛЬНЫ

МНЕНИЯ ОТНОСИТЕЛЬНО СИМПОЗИУМА «УСТРЕМЛЕНИЕ АФРИКИ – 2017»

ISTOCK

Капитан Домингос Таварес
Вооруженные Силы Кабо-Верде

ФОТОГРАФИИ РЕЙТЕР

Интернет и мобильные технологии находят в Африке широкое распространение, меняя все аспекты жизни на континенте и заставляя людей перебираться в киберпространство. Проблемы, связанные с внедрением цифровых технологий, очевидны, поскольку киберпреступники используют слабую законодательную базу в области кибербезопасности, а борьба с традиционными преступлениями требует транснационального взаимодействия. Симпозиум «Устремление Африки — 2017», проведенный в Малави, подчеркнул некоторые серьезные недостатки кибербезопасности, которые большинству стран на континенте еще предстоит рассмотреть. Высокопоставленные представители многих африканских стран участвуют в работе ежегодного симпозиума, организуемого совместно Африканским Командованием США и принимающей страной на ротационной основе.

Выступления участников вызвали активную дискуссию в аудитории и огромный интерес к пониманию не только параметров кибербезопасности, но и того, с чего же начать решение этих проблем. Автор этой статьи считает, что страны, такие как Кабо-Верде, которые уже начали решать вопросы кибербезопасности, должны быть готовы помогать другим странам, став партнерами в борьбе против киберпреступлений. Однако, главный шаг состоит в том, чтобы убедить политиков в важности вопросов кибербезопасности и необходимости создать законодательную базу, которая, если она будет соответствовать международным стандартам, будет эффективно бороться с киберпреступностью.

В ходе симпозиума представители Голландии наглядно проиллюстрировали, что угрозы для кибербезопасности часто начинаются с пользователя, чье невежество или беспечность могут открыть доступ к любой персональной информации на цифровых платформах. В выступлении была подчеркнута важность проявления бдительности при работе с отдельными вебсайтами, а также необходимость в надежном и безопасном пароле.

На конференции также обсуждалась природа международной организованной преступности, у которой сегодня появился компонент кибербезопасности. Государства сталкиваются с последствиями таких преступлений, как морское пиратство, незаконное рыболовство, а также незаконный провоз людей, животных и товаров. Установление связей и сотрудничество, поддерживаемые симпозиумами «Устремление Африки», цель которых в анализе и преодолении препятствий на пути к взаимодействию, могут сыграть фундаментальную роль в решении этих проблем.

В 2016 г. Кабо-Верде одобрила Национальную стратегию кибербезопасности, четко дав понять, что это основной фактор в развитии страны. Основная цель стратегии состоит в защите страны от киберугроз и преступлений путем распределения обязанностей между национальными, международными и общемировыми участниками.

Кибербезопасность является ключом к развитию, поскольку страна в огромной степени зависит от коммуникационных технологий, и ее уязвимость возрастает в результате этой зависимости. У нас есть структура электронного правления государственных органов, высокий процент пользователей интернетом (примерно 70% населения) и общество, которое переплетено коммуникационными сетями для личного пользования и для бизнес-операций.

Посетители интернет-кафе в Могадишу, Сомали, просматривают информацию в режиме онлайн, 2017 г. По мере развития коммуникационных технологий в Африке, стала насущной необходимость в механизмах кибербезопасности.

Граждане Тайваня и Китая, арестованные по подозрению в мошенничестве с телекоммуникационными сетями, слушают переводчика, Найроби, Кения. Угроза киберпреступлений возрастает по мере того, как в Африке распространяются цифровые технологии.

Стратегия охватывает вопросы кибербезопасности как для граждан, так и для общественных и частных организаций. Мы ясно даем понять, что Кабо-Верде не станет раем для киберпреступников, которых притягивают страны, где отсутствуют законные наказания за киберпреступления.

Наша страна развивает сотрудничество с Африканским Союзом и Экономическим сообществом стран Западной Африки и пользуется поддержкой партнеров, таких как США. Сейчас наша основная задача — создать национальный центр кибербезопасности, включающий группу реагирования на чрезвычайные компьютерные ситуации, которая будет предоставлять услуги во всех секторах, включая национальную оборону.

Киберпространство — это открытый мир, в котором преступник и совершенное им преступление совсем не обязательно находятся в одном и том же месте. Объектами нападения может быть гражданская, военная и полувоенная инфраструктура, и очевидно, что в последнее время различия между ними стираются. Таким образом, крайне важно, чтобы военные были в состоянии справляться с киберугрозами, которые снижают уровень безопасности, а также важно, чтобы происходил обмен информацией с цивилизованным миром, поскольку сотрудничество в цифровой среде просто необходимо.

Симпозиум «Устремление Африки — 2017» стал местом обсуждения вопросов национальной и региональной безопасности на африканском континенте. Он также остается прочным фундаментом для дальнейшего создания возможностей интеграции и взаимодействия для борьбы с интернет-угрозами, слабыми местами в кибербезопасности и постоянно меняющейся природой современной преступности. □

ДВОЙНОЙ ОБЪЕМ – ОНЛАЙН

Читайте новые и старые выпуски *per Concordiam*

http://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**

http://www.marshallcenter.org

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

Стационарные курсы

Democratia per fidem et concordiam

Демократия через доверие и дружбу

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

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

www.marshallcenter.org
registrar@marshallcenter.org

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

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.

ПАСС 19-19
10 Сентябрь -
20 Ноября 2019

Сентябрь

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

Октябрь

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

Ноябрь

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

ПРОГРАММА «БОРЬБА С ТРАНСНАЦИОНАЛЬНОЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ» (БТОП)

В центре внимания этой программы — резидентуры 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.

БТОП 19-6
12 Февраль -
7 Март 2019

Февраль

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

Март

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

БТОП 19-16
10 Июль -
1 Август 2019

Июль

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

Август

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

ПРОГРАММА «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.

ПТВБ 19-7
13 Март -
9 Апрель 2019

Март

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

Апрель

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

ПТВБ 19-18
7 Август -
4 Сентябрь 2019

Август

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

Сентябрь

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

ПРОГРАММА ПО ИЗУЧЕНИЮ ВОПРОСОВ КИБЕРБЕЗОПАСНОСТИ (ПВКБ)

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

ПВКБ 19-2
4-20 Декабрь 2018

Декабрь

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

СЕМИНАР ПО РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ (СРБ)

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

СРБ 19-8
24 Апрель - 17 Май 2019

Апрель

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

Май

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

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.

СВРС 19-15
24-28 Июнь 2019

Июнь

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

ПРОГРАММЫ ДЛЯ ВЫПУСКНИКОВ

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

Специалисты по связям с выпускниками

Дру Бек
Юго-Восточная Европа

Языки: английский, французский

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

Кристиан Эдер
Западная Европа

Языки: английский, немецкий

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

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

Языки: английский, русский, французский

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

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

Языки: английский, словацкий, итальянский, немецкий

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

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

Языки: английский, немецкий

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

mcalumni@marshallcenter.org

Подать материал для публикации

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

Подписаться

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

Найти нас

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

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

ФОТОГРАФИЯ ПРЕДОСТАВЛЕНА ЦЕНТРОМ ИМ. МАРШАЛЛА