Двусторонний проект Россия-США по кибербезопасности

Основы критически важной **терминологии**

Издание 1

Главные редакторы:

Карл Фредерик Раушер (Институт Восток-Запад),

Валерий Ященко (Институт проблем информационной безопасности МГУ имени М.В.Ломоносова).

Институт Восток-Запад является международной, негосударственной, некоммерческой организацией, главным образом занимающейся анализом критических вызовов, угрожающих миру. Институт Восток-Запад был основан в 1980 году с основной задачей ускорения процессов развития мер доверия, выработки направлений и развития сотрудничества. Институт имеет филиалы в Нью-Йорке, Брюсселе и Москве.

Контакты для получения дополнительной информации:
The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info
www.ewi.info

Институт проблем информационной безопасности (ИПИБ МГУ) создан 2 июля 2003 г. как обособленное структурное подразделение Московского государственного университета имени М.В.Ломоносова. Основной задачей Института является координация исследований в Московском университете, связанных с проблемами информационной безопасности, и организация международного научно-технического сотрудничества в этой сфере.

Контакты для получения дополнительной информации:
ИПИБ МГУ имени М.В.Ломоносова
119192, г. Москва,
Мичуринский проспект, 1, офис 10
+7 (495) 932-8958
iisi@iisi.msu.ru
www.iisi.msu.ru

Посвящается

Пионерам Российско-Американских отношений второй половины XX века, которым удалось предотвратить ужасный конфликт

Предисловие

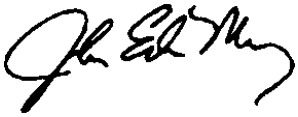
В течение прошлого года наблюдался бурный рост интереса к необходимости создать "правила дорожного движения" в киберпространстве. В отличие от суши, моря, воздуха и космоса, не существует общепринятых "правил дорожного движения" в киберпространстве. Первым шагом для продвижения в этом направлении является потребность закрепить в международном соглашении значение ключевых терминов. В течение ряда лет ООН и другие организации стимулировали усилия по согласованию базовой терминологии в сфере кибер- и информационной безопасности. Эти усилия были недостаточно активными и не принесли ожидаемых результатов. Многие призывают использовать для решения этой задачи потенциал экспертного академического сообщества.

Институт Восток-Запад в рамках своей Глобальной инициативы кибербезопасности и Институт проблем информационной безопасности МГУ согласились предпринять совместные усилия американских и российских экспертов для поиска консенсуса по терминологии в трех ключевых областях кибербезопасности, которые мы называем «Сфера действий», «Виды угроз» и «Типы действий». Наши эксперты создали эту концептуальную основу для обеспечения сложного процесса создания определений для общего международного словаря как необходимого этапа выработки "Правил дорожного движения".

Многие в Москве и Вашингтоне сомневались, что такие усилия могут увенчаться успехом. Четырнадцать наших коллег, под впечатляющим руководством Карла Раушера и Валерия Ященко, справились с этой задачей, предложив типологию и разработав первые двадцать терминов. Мы считаем, что эти усилия создали основу, опираясь на которую можно работать дальше – как в двустороннем формате между нашими странами, так и в многостороннем.

Мы благодарны за приглашение представить развёрнутый вариант этого доклада на Пятом международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» в апреле в городе Гармиш-Партенкирхен. Отзывы коллег на таком уважаемом форуме приветствуются, и будут использоваться для формирования нашей презентации на Втором глобальном саммите по кибербезопасности в Лондоне 1 и 2 июня 2011 года.

Мы с нетерпением ждем перехода этого проекта на следующий этап и надеемся, что наша работа стимулирует деятельность многих других, занимающихся этой тематикой, и способствует объединению международного сообщества для достижения так необходимого прорыва в кибер- и информационной безопасности.



Джон Эдвин Мроз
Президент и Исполнительный директор
Институт Восток-Запад

Владислав Петрович Шерстюк
Директор
Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

Введение

В настоящем документе собраны двадцать терминов, которые определяют кибер- и информационную безопасность. Основная задача этой работы состояла в том, чтобы начать давно назревшие обсуждения всеобъемлющих "правил дорожного движения" в киберпространстве в части опасных конфликтов, имеющих самые серьезные последствия.

Есть пять веских причин, почему именно Россия и Соединенные Штаты являются идеальными партнерами для начала такой инициативы. Во-первых, на протяжении большей части прошлого века холодная война между нашими двумя странами определяла ход мировой политики. Отсюда следует, второе, а именно оценки, проведенные нашими странами друг о друге, были достаточно успешными, чтобы избежать страшного, немыслимого гарантированного взаимного уничтожения. На самом деле, историческим фактом является то, что наши две страны никогда не были в состоянии («горячей») войны друг с другом. В-третьих, Россия и Америка являются сверхдержавами в киберпространстве, которые в течение долгого времени задавали тон в передовых научно-технических открытиях и проектах. В-четвертых, наши две страны, охватывая три континента, олицетворяют собой очень разнообразные истории и идеологии и придерживаются активной точки зрения на мир. Наконец, и Россия, и Америка заинтересованы в глобальной стабильности, процветании и мире.

Мы оба благодарны участникам нашей команды, каждый из которых – специалист мирового класса в рассматриваемой области.

Эти термины выносятся для обсуждения и корректировки широким международным сообществом. Эта таксономия будет представлена на Пятом международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» в этом месяце в городе Гармиш-Партенкирхен, Втором глобальном саммите кибербезопасности в июне в Лондоне и Конференции по глобальной безопасности в октябре этого года в Брюсселе. Кроме того, на протяжении всего этого процесса ожидаются консультации с членами группы Института Восток-Запад Кибер40 и Международным исследовательским консорциумом по информационной безопасности.

Успехов в дискуссиях!

Карл Фредерик Раушер
Руководитель группы экспертов США
Старший специалист по технологиям и
Ведущий сотрудник Института Восток-Запад

Нью-Йорк, США

Валерий Ященко
Руководитель группы экспертов России
Заместитель директора
Института проблем информационной безопасности
МГУ имени М.В.Ломоносова

Москва, Россия

Авторы[1]

Российская Федерация
Russian Federation

Сергей Комов, ИПИБ МГУ

Андрей Кульпин, ИПИБ МГУ

Алексей Сальников, ИПИБ МГУ

Анатолий Стрельцов, аппарат Совета Безопасности Российской Федерации

Владимир Иванов, Институт Восток-Запад

Соединенные Штаты Америки
United States of America

Чарльз Барри, Национальный Университет обороны

Джон С. Эдвардс, корп. Digicom

Гиб Гудвин, контр-адмирал ВМС США (в отставке), Northrop Grumman

Стюарт Голдман, бывший исследователь Bell Labs

Пол Николас, корп. Microsoft

Джеймс Брет Майкл, Школа повышения квалификации офицерских кадров ВМС США

Джек Ослунд, Университет им. Джорджа Вашингтона

[1] Для краткой биографической справки см. Приложение

Благодарности

Особое признание и искреннюю благодарность мы выражаем:

Вартану Саркиссяну и Владимиру Иванову

За их видение и настойчивость в развитиии этого начинания

Францу-Стефану Гади

За управление взаимодействием в проекте и активный анализ политической составляющей

Эндрю Нагорски, Трэйси Ларсен, Драгану Стояновски и Эбигэйл Рабинович

За контроль качества издания и управление процессами коммуникации

Грегу Остину и Терри Моргану
За их постоянную поддержку и поощрение двусторонней российско-американской программы

Карасеву Павлу
За активное участие в подготовке русскоязычной версии издания

Анатолию Сафонову, Владиславу Шерстюку, Андрею Крутских, Сергею Кисляку, Уильяму Бернсу, Майклу МакФаулу, Джону Бейрлу, Дону Кендалу старшему и Джону Эдвину Мрозу
за их дальновидность и поощрение таких неформальных русско-американских совместных усилий по противодействию наиболее сложным глобальным проблемам безопасности

наконец, более широкому сообществу заинтересованных людей в Москве, Вашингтоне и во всем мире, чей интерес и признательность за инновации в этом процессе подтверждает его полезность в долгосрочной перспективе.

1. Введение

Давно пришла пора внести ясность в понимание проблем киберпространства, имеющих большую политическую значимость для государств. Действительно, существует неприемлемая путаница в отношении смысла даже самых базовых терминов – киберпространство, кибервойна, кибератака и т.д. Учитывая важность событий, произошедших в киберпространстве в последние нескольких лет, резонно полагать, что в любой момент интерпретация одного из этих терминов может оказаться решающим моментом в определении того, приведут ли действия в киберпространстве к росту эскалации или насилию.

Россия и Соединенные Штаты составляют идеальное партнерство для реализации инициативы по созданию начального импульса классификации терминов. Среди прочего, обе страны уважаемы за компетентность в данной области, опыт управления ядерным противостоянием, и приверженность интересам содействия глобальной стабильности, процветанию и миру.

Этот документ является реальным шагом вперед на пути к выработке ясной таксономии киберконфликта. Работа имеет целью стимулировать многостороннее сотрудничество по данному вопросу.

Цели и значение

Для этого двустороннего взаимодействия были установлены три цели. Первая цель заключалась в том, чтобы *начать реальный диалог* экспертов и уполномоченных лиц обеих стран. Вторая цель, основанная на первой, заключается в выработке более глубокого понимания точек зрения обеих стран. Третья цель заключается в достижении консенсуса по поводу определений критически важных терминов в сфере кибер и информационной безопасности[2]. Созданная таксономия выносится для рассмотрения, анализа и улучшения, таким образом, термины могут быть уточнены и использованы в официальных соглашениях между двумя странами, а также могут быть использованы в качестве ориентира другими государствами.[3] Первые две цели были достигнуты, как это явствует из содержания этого доклада. Но нужно время, чтобы определить успехи для движения к третьей цели.[4]

Причины для начала совместной разработки терминологии по кибербезопасности совершенно ясны. Многие эксперты и уполномоченные лица во всем мире придерживаются мнения, что давно назрел момент принятия международных соглашений, или "правил дорожного движения".[5]

Представителями США этот проект в рамках экспертного сообщества рассматривается как реальное наполнение новой политике в киберпространстве. В обзоре политики США в киберпространстве 2009 года был изложен ряд приоритетных направлений, и международное сотрудничество указано седьмым пунктом "плана действий на ближайшее время". В частности, была поставлена задача "укрепления наших международных партнерств для создания инициатив, направленных на развитие всего комплекса мероприятий, политик и возможностей, связанных с кибербезопасностью."[6]

Для представителей России, это двустороннее сотрудничество рассматривается, как выполнение предложенных Организацией Объединенных Наций рекомендаций по систематизации терминов. Российские эксперты ссылаются на Доклад 2010 года Группы ООН правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности,

[2] Словосочетания «кибер и информационная безопасность», а также «информационная и кибер безопасность» были согласованы совместно и относятся к более широкому кругу интересов. В этих словосочетаниях, слова «кибер» и «безопасность» намеренно разделены с целью распараллеливания конструкций, а также соответствующих интересов. Во всех иных случаях употребляется слово «кибербезопасность».

[3] То есть в ходе официальных переговоров

[4] На момент публикации планы по расширению диалога и внедрения приведенных в настоящем документе рекомендаций разрабатываются.

[5] Данные опроса участников Первого Глобального саммита по кибербезопасности в Далласе, май 2010 года.

[6] Обзор политики в киберпространстве Белого Дома; Таблица 1: План действий на период президентства, Вашингтон, 2009 год, стр. vi

который рекомендовал предпринять «дальнейшие шаги по разработке мер укрепления доверия и прочих мер в целях снижения риска возникновения неправильного восприятия в результате дезорганизации или нарушений, связанных с применением ИКТ: ... (V) нахождение возможностей для выработки общей терминологии и определений в связи с положениями резолюции 64/25 Генеральной Ассамблеи»[7].

Таким образом, задача состоит не в гармонизации существующих терминологий, в избытке представленных в различных национальных документах (стандартах, национальных законах и т.д.). Существенно более масштабная цель включает в себя укрепление доверия, развитие подлинного понимания и положительного импульса для реализации более широкомасштабных действий для создания "правил дорожного движения".

Ожидается, что эти термины будут использованы, в первую очередь, в более широком международном сотрудничестве по определению ключевых терминов и создания общей классификации. Таким образом, эти термины не имеют обязательной силы, а скорее обеспечивают привлечение уполномоченных политиков разных стран к решению этой важной и назревшей задачи. Проявление их значимости в ближайшие годы будет заключаться во взаимном сближении точек зрения по общим определениям. В равной мере большое значение имеет более четкое проявление тех вопросов, где остаются неразрешимые разногласия.

Этот первый шаг действительно имеет большое значение, поскольку он родился в ходе российско-американского сотрудничества и потому, что это является явным движением вперед.

Информация и Киберпространство

Одним из наиболее значительных препятствий на пути двусторонних обсуждений, которое предстояло решить, было принципиальное разногласие по поводу отправной точки для работы. Существовало две точки зрения:

Российская точка зрения на информационную безопасность делает акцент на всеобъемлющем характере информации, где киберпространство является только одним из элементов системы. Информация рассматривается как естественная и искусственная. Киберпространство является искусственной средой, и рассматривается как техническое измерение информации. Кроме кибер, информация также включает в себя мысли в человеческом сознании и информацию в книгах и документах. Таким образом, делается логический вывод, что дискуссия должна охватывать всю информацию, а не только её часть, то есть кибер.

В русском языке наиболее точным эквивалентом английского "security" является "защита". Точка зрения России на **безопасность информации** включает в себя несколько аспектов: гуманитарные, социальные, духовные и технические факторы (т.е. кибер). Также одним из важнейших аспектов «информационной безопасности» является защита населения от терроризма и цензуры.[8]

Американцы больше заинтересованы в рассмотрении данных, появляющихся в электронных инфраструктурах. Они признают существование информации вне киберпространства, но считают, что в настоящий момент это направление не приоритетно. В ходе двусторонней работы они хотели сконцентрировать внимание на том, что возникает в киберпространстве. Помимо этого, были и другие причины, почему американцы были заинтересованы в рассмотрении именно "кибербезопасности". В частности, американцы не рассматривают защиту информации, как нечто, что должно включать цензуру, или любую попытку контроля информированности населения. Идея заключается в том, что для защиты населения от вредной информации наилучшим образом подходит повышение уровня образованности и осведомленности. Наконец, американская команда считает, что это будет неправильно, если правительство начнет использовать психологические операции на своих гражданах.

Признавая эти различия во взглядах, была достигнута договоренность ограничить обсуждение терминами «кибер», которые были признаны обеими командами экспертов составной частью более широкого понятия

[7] http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201
[8] Критически важное информационное пространство определяется как совокупность элементов информационного пространства, которые рассматриваются жизненно необходимыми национальными правительствами или международными соглашениями.

"информация". В частности, стороны достигли согласия, когда признали (i) расширенную трактовку понятия «информация, (ii) признали, что термин "кибер" является подмножеством этого более широкого круга понятий, и (iii) согласились ограничиться вопросом, связанным с кибер-, так как эта область требует наибольшего внимания.

Предмет исследования

Есть три параметра, которые лучше всего определяют предмет дискуссии. Они заключаются в том, что:

1. Сторонами, принимающими участие в первоначальном исследовании, являются Россия и США;[9]
2. Рассматривается «информационная и кибер- безопасность», при этом начальное обсуждение ограничивается последним;
3. Целью работы является разработка определений и классификации для использования в многосторонних переговорах.

[9] Эта работа была проведена экспертами из России и США. Каждый эксперт является гражданином представляемой им страны и принимал участие в проектах, связанных с обеспечением интересов национальной безопасности. Ввиду того, что эта работа проходит в формате обсуждений на уровне экспертов, участники не являются официальными представителями государственной власти. Руководители обеих экспертных групп регулярно информировали уполномоченным лиц в Москве и Вашингтоне. Совместный опыт экспертов превышает несколько сот лет и содержит знания, необходимые для исследования рассматриваемого предмета.

2. Согласованные определения

В этом разделе представлены двадцать терминов, по которым российские и американские эксперты пришли к согласию. Термины разбиты на три группы: сфера действий, виды угроз и типы действий.

Сфера действий

- Киберпространство
- Киберинфраструктура
- Киберсервисы
- Критически важное киберпространство
- Критически важная киберинфраструктура
- Критически важные киберсервисы

Виды угроз

- Киберпреступность
- Кибертерроризм
- Киберконфликт
- Кибервойна
- Кибербезопасность

Типы действий

- Боевые действия в киберпространстве
- Кибератака
- Киберконтратака
- Оборонительные средства противодействия в киберпространстве
- Кибероборона
- Оборонительные возможности в киберпространстве
- Наступательные возможности в киберпространстве
- Использование преимуществ в киберпространстве
- Средства кибersдерживания

Сфера действий

В этом разделе представлены шесть согласованных определений, а именно: киберпространство, киберинфраструктура, киберсервисы, критически важное киберпространство, критически важная киберинфраструктура, критически важные киберсервисы. Каждый из первых трех терминов имеет критически важное измерение, которое составляет три последних определения.

Взаимосвязь между киберпространством, киберинфраструктурой и киберсервисами трудно показать в простой графической форме без искажения смысла. Киберпространство построено на киберинфраструктуре. Киберсервисы придают киберпространству интерес и ценность для пользователей. Киберсервисы функционируют с помощью систем, из которых состоит киберинфраструктура.

Далее представлены шесть определений.

Cyberspace[10]

is [a]an electronic medium through which [b]information is [c]created, [d]transmitted, [e]received, [f]stored, [g]processed, and [h]deleted.

Киберпространство

[а]электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация [б]создаётся, [в]передаётся, [г]принимается, [д]хранится, [е]обрабатывается [ж]и уничтожается.

[10] Комментарий

Необходимо учитывать следующие важные аспекты

Кибер происходит от греческого слова κυβερνητικός – и означает искусство управления. Термин «кибернетика» был введен в книге Норберта Винера «Кибернетика, или Управление и связь в животном и машине». Автор применил этот термин к миру животных и механическим сетям в контексте контроля сложных систем. В дальнейшем, термин начал использоваться в медицинском сообществе в отношении взаимодействия людей и животных с механизмами. Тем не менее, с момента своего появления, термин получил ряд значений. Термин эффективно используется в науке, бизнесе, праве и политике. Сейчас этот термин полезен тем, что может с готовностью быть использован для определения отличного от физического, виртуального мира, созданного Интернетом и электронными средствами связи.

С другой стороны, киберпространство не существует без физической компоненты.

Использование в термине слова «пространство» подразумевает наличие определенного измерения. Таким образом, киберпространство занимает некий объём. Также, киберпространство рядом людей приравнивается к суше, водному и воздушному пространству, а также космосу. Однако, если эти среды являются естественными, то киберпространство – искусственно создано человеком.

В процессе составления определения были рассмотрены существующие дефиниции. Министерство Обороны США определяет киберпространство, как «глобальное пространство в цифровой среде, состоящее из взаимозависимых сетей информационно-коммуникационных инфраструктур, в том числе Интернета, сетей связи, компьютерных сетей и встраиваемых процессоров и контроллеров». См. Словарь военных и связанных терминов; изд. Министерства Обороны США, 31 января 2011 года, стр. 92-93

Cyber Infrastructure[11]

is [a]the aggregation of people, processes and systems [b]that constitute **cyberspace.**

Киберинфраструктура

[а]совокупность людей, процессов (в том числе управляющих), [б]и систем, составляющих киберпространство

[11] Комментарий

Необходимо учитывать следующие важные аспекты

Киберинфраструктура состоит из восьми необходимых частей: Среда (здания, места расположения вышек сотовой связи, орбиты спутников, морское дно, где пролегают кабели связи, и т.д.), Энергия (электричество, батареи, генераторы, и т.д.), аппаратное обеспечение (полупроводниковые микросхемы, магнитные карты и печатные платы, системы проводной и оптоволоконной передачи данных), Программное обеспечение (исходные коды, скомпилированные программы, системы контроля и управления версиями, базы данных, и т.д.), Сети (узлы, соединения, топология сети, и т.д.), Передачи (информация, передаваемая посредством сетей, статистика и схемы передачи трафика, перехват данных, порча данных, и т.д.), Персонал (инженеры, разработчики, операторы, обслуживающий персонал, и т.д.), и Политика, или в развернутом виде Соглашения, Стандарты, Политики и Нормативные документы. Карл Раушер, «Защита инфраструктуры связи», Технический журнал лабораторий Bell – Спец выпуск: Внутренняя безопасность, Том 9, Выпуск 2, 2004 год.

Тенденцией во всем мире становится рост зависимости существующей инфраструктуры от компьютеров и информационных сетей, и их большая интеграция в киберпространство.

В процессе выработки определения использовались существующие дефиниции.

Cyber Services[12]

are [a] a range of data exchanges in cyberspace [b] for the direct or indirect benefit of humans.

Киберсервисы (услуги, службы)

[а] различные виды обмена данными в киберпространстве, [б] для прямой или косвенной пользы людям

[12] Комментарий

Необходимо учитывать следующие важные аспекты

Киберсервис оказывается посредством приложения. Это приложение может быть предоставлено через киберпространство посредством процессов и данных. Это означает, что системы могут находиться в различных действительно существующих географических местоположениях.

Киберсервисы могут оказываться как при подключении к сети, так и без него, обрабатываться локально или удаленно, в режиме реального времени, или с задержкой передачи данных или обработки.

Киберсервисы не следует рассматривать, как окончательную концепцию, так как многие ожидаемые сервисы ещё не были разработаны (например, в потенциал версии 6 Интернет-протокола входит значительное увеличение числа подключенных пользователей).

В процессе выработки определения использовались существующие дефиниции.

Critical Cyberspace[13]

is [a] **cyber infrastructure** and **cyber services** that are vital to preservation of [c]public safety, [d]economic stability, [e]national security [f]and international stability

Критически важное киберпространство

[а][часть (элементы) киберинфраструктуры и киберуслуг], которые необходимы для осуществления, [б]жизненно важных функций поддержания, [в]общественной безопасности, [г]экономической стабильности, [д]национальной безопасности, [е]международной стабильности

[13] Комментарий

Этот термин представлет собой подвид киберпространства

В процессе выработки определения использовались существующие дефиниции.

Critical Cyber Infrastructure[14]

is [a] the **cyber infrastructure** that is essential to [b] vital services for [c] public safety, [d] economic stability, [e] national security, [f] international stability and [g] to the sustainability and restoration of **critical cyberspace.**

Критически важная киберинфраструктура

[а] киберинфраструктура, которая необходима для, [б] осуществления жизненно важных функций, [в] поддержания общественной безопасности, [г] экономической стабильности, [е] национальной безопасности, [ж] международной стабильности, ([з]) а также для поддержания работоспособности и функций эффективного восстановления [критически важного киберпространства

[14] Комментарий

Необходимо учитывать следующие важные аспекты

Наиболее критически важными инфраструктурами являются системы, которые обеспечивают функционирование связи, энергетики, транспорта, финансовой системы и правительства. Таким образом, информационно-коммуникационые системы, необходимые для базового функционирования этих отраслей, являются критически важными.

Некоторые страны являются более зависимыми от критически важной киберинфраструктуры, чем другие. Отчасти это происходит по причине роста сложности таких систем, но также и по причине отсутствия не высокотехнологичных резервных возможностей.

В процессе выработки определения использовались существующие дефиниции.

Critical Cyber Services[15]

are [a]**cyber services** that are vital to [b]preservation of [c]public safety, [d]economic stability, [e]national security [f]and international stability.

Критически важные Киберсервисы (услуги, службы)

[а]часть (элементы)] киберсервисов (услуг, служб), которые необходимы для осуществления, [б]жизненно важных функций поддержания , [в]общественной безопасности, [г]экономической стабильности, [д]национальной безопасности, [е]международной стабильности

[15] Комментарий

Этот термин представлет собой подвид киберсервисов

В процессе выработки определения использовались существующие дефиниции.

Виды угроз

В этом разделе представлены согласованные определения пяти терминов, а именно: киберпреступность, кибертерроризм, киберконфликт, кибервойна и кибербезопасность. Последний термин – противоположность эскалации конфликта.

Главной отличительной чертой киберпреступности является нарушение законов. Подобным образом, отличительной чертой кибервойны является участие политических акторов. Киберконфликт находится в одной плоскости с войной, но располагается ниже критической черты.

Далее приведено пять определений.

Cyber Crime[16]

is [a]the use of **cyberspace** [b]for criminal purposes [c]as defined by national or [d]international law.

Киберпреступление

[а]использование киберпространства, [б]в преступных целях, [в]которые определяются в качестве таковых национальным или международным законодательством

[16] Комментарий

Необходимо учитывать следующие важные аспекты

Учитывая наличие значительного количества существующих законов, которые содержат описание неправомерных действий, термин Киберпреступление намеренно определен таким образом, чтобы содержать ссылку на существующие правовые конструкции.

Подразумевается, что юридические факторы, которые необходимо учитывать, играют неотъемлемую роль в применении этого термина. Трудности возникают, когда индивид в одной стране использует киберресурсы во второй стране для оказания воздействия на человека, организацию или иного актора в третьей стране.

Киберпреступники всё чаще признаются влиятельными негосударственными акторами.

Конвенция по Киберпреступности 2001 года является первым международным договором, который направлен на гармонизацию законодательств различных стран в сфере киберпреступлений. Он был составлен Советом Европы с участием США в качестве наблюдателя. США ратифицираовали договор, а Россия нет.

В процессе выработки определения использовались существующие дефиниции.

Cyber Terrorism[17]

is [a]the use of **cyberspace** [b]for terrorist purposes [c]as defined by national or [d]international law.

Кибертерроризм

[а]использование киберпространства, [б]в террористических целях, [в]которые определяются в качестве таковых национальным или международным законодательством

[17] Комментарий

Необходимо учитывать следующие важные аспекты

Учитывая наличие определенного прогресса в поиске определения терроризма, термин Кибертерроризм намеренно определен таким образом, чтобы опираться на существующие достижения.

Подразумевается, что юридические факторы, которые необходимо учитывать, играют неотъемлемую роль в применении этого термина. Трудности возникают, когда индивид в одной стране использует киберресурсы во второй стране для оказания воздействия на человека, организацию или иного актора в третьей стране.

В процессе выработки определения использовались существующие дефиниции.

Cyber Conflict[18]

is [a]tense situation [b]between or among nation-states or organized groups [c]where unwelcome **cyber attacks** [d]result in retaliation.

Киберконфликт

[а]напряженная ситуация между и/или среди государств и/или политически организованных групп, [б]при которой враждебные (нежелательные) кибератаки, [в]провоцируют (приводят) к ответным действиям.

[18] Комментарий

Необходимо учитывать следующие важные аспекты

Кибератаки могут включать в себя физическое воздействие на киберинфраструктуру.

Методы ответа на атаку могут быть асимметричными (то есть кибер, физические). Таким образом, ответ может реализовываться не только через киберпространство. Таким же образом, атаке не обязательно быть в киберпространстве, чтобы вызвать ответные действия через киберпространство.

Киберконфликт может быть предвестником эскалации напряженности.

В процессе выработки определения использовались существующие дефиниции.

Cyber War[19]

is [a]an escalated state [b]of **cyber conflict** [c]between or among states [d]in which **cyber attacks** [e]are carried out by state actors [f]against **cyber infrastructure** [g]as part of a military campaign

[h](i) Declared: that is formally declared by an authority of one of the parties.

(ii) De Facto: with the absence of a declaration.

Кибервойна

[а]высшая степень киберконфликта, [б]между или среди государств, [в]во время которой государства предпринимают кибератаки, [г]против киберинфраструктур противника, [д]как часть военной кампании;

[е](i) может быть объявлена формально одной (всеми) конфликтующими сторонами или

(ii) не объявляться формально и быть *de facto*

[19] Комментарий

Необходимо учитывать следующие важные аспекты

Война существует как состояние между или среди враждующих групп.

Война, как правило, проходит различные этапы. Киберконфликт, как правило, предшествует Кибервойне.

Существует тенденция включать боевые действия в киберпространстве в состав конвенциональной войны.

В случае отсутствия политических акторов, отсутствует и война. Кибервойна не ограничивается только военными операциями, особенно в отношении начального этапа, например, проявляется в виде разведывательных операций. Кибервойна может проводиться различными группами по-разному.

В процессе выработки определения использовались существующие дефиниции. Недавний доклад двусторонней российско-американской группы института Восток-Запад предложил концепцию действий «иных, чем война» [см. Рекомендацию 5 издания «Выработка правил поведения в киберконфликте – применимость Женевской и Гаагской конвенций в киберпространстве», Карл Раушер, Андрей Коротков, Двусторонняя российско-американская группа по защите критически важной инфраструктуры института Восток-Запад, январь 2011 года]

Cybersecurity[20]

is [a]a property of **cyber space** [b]that is an ability to resist [c]intentional and unintentional threats [d]and respond and recover.

Кибербезопасность

[а]свойство (киберпространства, киберсистемы), [б]противостоять, [в]намеренным и/или, [г]ненамеренным угрозам, а также, [д]реагировать на них и, [е]восстанавливаться после воздействия этих угроз.

[20] Комментарий

Важные аспекты обсуждаются в параграфе «информация и кибер» первой части.

Слово «безопасность» в русском языке обозначает защищенность, но в него не включаются дополнительные значения этого слова в английском языке, например, средства обеспечения безопасности.

В процессе выработки определения использовались существующие дефиниции. Интерес представляет исследование, подчеркивающее ориентацию концепции защищенности вокруг чувства нахождения в безопасности.

Типы действий

В данном разделе представлены согласованные определения девяти терминов, а именно: боевые действия в киберпространстве, кибератака, киберконтратака, оборонительные средства противодействия в киберпространстве, кибероборона, оборонительные возможности в киберпространстве, наступательные возможности в киберпространстве, использование преимуществ в киберпространстве, средства киберсдерживания.

Особо отмечено, что не представлен ещё один ключевой термин - "кибероружие". Это имеет большое значение, потому что некоторые из определений ссылаются на него. Таким образом, этот термин находится в центре внимания следующего этапа настоящей работы.[21]

Далее представлено девять определений.

[21] Двусторонняя российско-американская группа по защите критически важной инфраструктуры института Восток-Запад недавно предложила значительное количество определений кибероружия в контексте системы четырех переменных, относящихся к типу инфраструктуры и типу оружия. Отдельным наблюдением этой дискуссии является вывод, что кибероружием являются как чисто информационно-коммуникационные средства, так и насыщенные информационно-коммуникационными технологиями виды конвенционального оружия. [см. Секцию 3 издания «Выработка правил поведения в киберконфликте – применимость Женевской и Гаагской конвенций в киберпространстве», Карл Раушер, Андрей Коротков, Двусторонняя российско-американская группа по защите критически важной инфраструктуры института Восток-Запад, январь 2011 года]

Cyber Warfare[22]

is [a]**cyber attacks** [b]that are authorized by state actors [c]against **cyber infrastructure** [d]in conjunction with a government campaign.

Боевые действия в киберпространстве

[а]кибератаки, [б]проводимые государствами (группами государств, организованными политическими группами), [в]против киберинфраструктур, [г]и являющиеся частью военной кампании

[22] Комментарий

Необходимо учитывать следующие важные аспекты

Боевые действия в киберпространстве относятся к действиям или средствам воздействия, применяемым участниками конфликта.

В процессе выработки определения использовались существующие дефиниции.

Cyber Attack[23]

is [a] an offensive [b] use of a **cyber weapon** [c] intended to harm a designated target.

Кибератака

[а] наступательное, [б] использование [кибероружия], [в] с целью нанесения вреда определенной цели

[23] Комментарий

Необходимо учитывать следующие важные аспекты

Слово «вред» включает в себя приведение в упадок, воспрещение действий – временно или постоянно.

Атака в том случае является эффективной, если использует внутренние неотъемлемые уязвимости цели.

Кибератака определяется типом используемого оружия, а не природой цели. Таким образом, кибератакой может быть как применение кибероружия против киберсредств, так и против целей в физическом мире. Но кибератакой не является применение не-кибероружия против киберсредств или против целей в физическом мире. См. предыдущие сноски для получения дополнительных сведений.

Среди вопросов, на которые совместная команда не смогла найти ответа, есть следующий: является ли кибератакой применение пропаганды, захват контроля над веб-сайтом, действия с использованием электронной почты.

В процессе выработки определения использовались существующие дефиниции. Агентство НАТО по стандартизации определяет «атаку на компьютерные сети» как «Действия, предпринимаемые с целью нарушения доступа к информации, хранящейся на компьютере, её порчи или удаления»; дополнительно отмечено: «Атака на компьютерные сети является разновидностью кибератаки». «Словарь терминов и определений НАТО», 22 января 2010 года, стр. 2-С-12. Это единственное упоминание слова «кибер» в публикации НАТО. В соответствии с правилами, упоминание этого определения в настоящей публикации было отправлено в Агентство НАТО по стандартизации.

Cyber Counter-Attack[24]

is [a]the use of a **cyber weapon** [b]intended to harm a designated target [c]in response to an attack.

Киберконтратака

[а]использование, [б]кибероружия с целью нанесения вреда определенной цели, [в]в ответ на атаку

[24] Комментарий

Необходимо учитывать следующие важные аспекты

Киберконтратака может быть асимметричной. Таким образом, киберконтратакой может быть как применение кибероружия против киберсредств, так и против целей в физическом мире. Но киберконтратакой не является применение не-кибероружия против киберсредств или против целей в физическом мире. Таким образом, подобно кибератаке, она определяется не типом цели, а видом используемого оружия.

В процессе выработки определения использовались существующие дефиниции.

Cyber Defensive Countermeasure[25]

is [a]the deployment [b]of a specific **cyber defensive capability** [c]to deflect [d]or to redirect [e]a **cyber attack**.

Оборонительные средства противодействия в киберпространстве

[а]развертывание особых (оборонительных средств противодействия) [б]для отражения и/или, [в]перенаправления кибератаки

[25] Комментарий

Необходимо учитывать следующие важные аспекты

Включение этого термина в исходную классификацию, имеющую отношение к защите, чрезвычайно важно, поскольку позволяет объяснить законное право государств тратить средства на разработку средств, которые могут понадобиться при защите их интересов.

Оборонительные средства противодействия в киберпространстве – это действия, предпринимаемые в интересах одной из сторон, как часть оборонительной стратегии во время или после атаки.

Оборонительные средства противодействия могут быть как пассивными, так и активными. Реакция активных средств может заключаться в попытке выведения атакующей стороны из строя. Пассивные средства могут повышать уровень защиты интересов одной из сторон.

В процессе выработки определения использовались существующие дефиниции.

Cyber Defense[26]

is [a]organized capabilities [b]to protect against, [c]mitigate from, and [d]rapidly recover from [e]the effects of **cyber attack**.

Кибероборона

[а]организованная совокупность средств и действий, [б]для защиты и/или, [в]для смягчения, [г]и эффективного восстановления, [д]от враждебных кибератак (воздействий)

[26] Комментарий

Необходимо учитывать следующие важные аспекты

Кибероборона относится к действиям, предпринимаемым одной из сторон в ожидании атаки для защиты своих интересов. Включение этого термина в исходную классификацию, имеющую отношение к защите, чрезвычайно важно, поскольку позволяет объяснить законное право государств тратить средства на разработку средств, которые могут понядобиться при защите их интересов.

Эффективная оборона в электронных системах основывается, как правило, на обнаружении, изоляции, уведомлении, восстановлении и нейтрализации.

Эффективной стратегией кибероборонs может быть поглощение атаки.

Атака в том случае является эффективной, если использует внутренние неотъемлемые уязвимости цели.

В процессе выработки определения использовались существующие дефиниции.

Cyber Defensive Capability[27]

is [a]a capability [b]to effectively protect [c]and repel [d]against a cyber exploitation or [e]cyber attack, [c]that may be used as a **cyber deterrent**.

Оборонительные возможности в киберпространстве

[а]возможность эффективно защитить и/или, [б]отразить, [в]кибератаку, предотвратить киберконфликт, предупредить использование противником преимуществ в киберпространстве, [г]и которая может быть использована в качестве средства сдерживания в киберпространстве

[27] Комментарий

Необходимо учитывать следующие важные аспекты

Включение этого термина в исходную классификацию, имеющую отношение к защите, чрезвычайно важно, поскольку позволяет объяснить законное право государств тратить средства на разработку средств, которые могут понадобиться при защите их интересов.

В процессе выработки определения использовались существующие дефиниции.

Cyber Offensive Capability[28]

is [a]a capability [b]to initiate [c]a **cyber attack** [d]that may be used [e]as a **cyber deterrent**.

Наступательные возможности в киберпространстве

[а]возможность начать, [б]кибератаку, [в]которая может быть использована в качестве средства сдерживания в киберпространстве

[28] Комментарий

Необходимо учитывать следующие важные аспекты

В процессе выработки определения использовались существующие дефиниции. В Министерстве Обороны США используется родственный термин: «операции в киберпространстве», которые определяются как «использование киберсредств там, где первоочередной задачей является достижение цели в/или посредством киберпространства. К таким операциям также относятся операции в компьютерных сетях и действия по управлению и защите глобальной информационной сети». См. Словарь военных и связанных терминов; изд. Министерства Обороны США, 31 января 2011 года, стр. 92-93

Cyber Exploitation[29]

is [a]taking advantage [b]of an opportunity [c]in **cyber space** [d]to achieve an objective.

Использование преимуществ в киберпространстве

[а]использование в своих интересах, [б]имеющихся возможностей в киберпространстве, [в]для достижения поставленной цели

[29] Комментарий

Необходимо учитывать следующие важные аспекты

Под преимуществом здесь понимается либо сила атакующей стороны, либо уязвимость другой стороны.

Участники российской команды уточняют, что этот термин в России не используется.

В процессе выработки определения использовались существующие дефиниции. Агентство НАТО по стандартизации определяет «использование преимуществ в киберпространстве» как «Действия по использованию компьютеров или компьютерных сетей, равно как и хранящейся в них информации, для получения преимуществ». «Словарь терминов и определений НАТО», 22 января 2010 года, стр. 2-С-12. Это единственное упоминание слова «кибер» в публикации НАТО. В соответствии с правилами, упоминание этого определения в настоящей публикации было отправлено в Агентство НАТО по стандартизации.

Cyber Deterrent[30]

is [a]a declared [b]mechanism [c]that is presumed effective [d]in discouraging **cyber conflict** [e]or a threatening activity [f]in **cyberspace**.

Средства киберсдерживания

[а]признанный, [б]механизм, [в]который считается действенным, [г]для препятствования, [д]киберконфликту, [е]или угрожающей деятельности в [киберпространстве]

[30] Комментарий

Необходимо учитывать следующие важные аспекты

В механизмы средств киберсдерживания включаются политика, военно-стратегическая концепция, оружие, средства, альянсы.

В процессе выработки определения использовались существующие дефиниции.

3. Дальнейшие действия

Это совместный документ содержит двадцать согласованных терминов, которые были подготовлены экспертами из России и Соединенных Штатов. Эти термины являются одними из наиболее важных для определения и понимания "правил поведения" в конфликтных ситуациях в развивающемся кибер и информационном пространстве. На протяжении десяти лет предпринимались многочисленные попытки выработать совместный русско-американский глоссарий терминов для киберпространства. По ряду причин они зашли в тупик. Этот проект является первым, принесшим ожидаемые результаты. Наша совместная команда многое сделала для разработки этой классификации, и надеется, что она может быть улучшена в ближайшие месяцы и годы. Несмотря на то, что двадцать терминов – немного, в сравнении с большинством словарей, эти термины являются значительным шагом, так как открывают начало пути.

Дальнейшие шаги включат детальное рассмотрение понятий "информация" и "информационная безопасность" и определение связи между ними. Следующие шаги также включают расширение круга участников и преобразование обсуждения в многостороннее. Это означает получение отзывов от группы Кибер40 Института Восток-Запад и Международного Исследовательского Консорциума Информационной Безопасности (МИКИБ). Среди запланированных многосторонних мероприятий можно выделить:

- Пятый Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» в апреле этого года в городе Гармиш-Партенкирхен;
- Проводимый институтом Восток-Запад и Институтом инженеров по электронике и электротехнике Второй глобальный саммит по Кибербезопасности в июне этого года в Лондоне;
- Конференция института Восток-Запад по безопасности в октябре этого года в Брюсселе.

Команда надеется на развитие дальнейшего сотрудничества, на дальнейшее развитие представленной классификации, огромная важность которой подчеркивается отсутствием на данный момент каких-либо ориентиров в кибер и информационном пространстве.

БИОГРАФИИ

Главные редакторы

Карл Фредерик Раушер

Карл Фредерик Раушер является Главным директором по технологиям и заслуженным сотрудником Института Восток-Запад. Ранее он работал исполнительным директором Управления по повышению надежности и безопасности сетей лабораторий Bell компании Alcatel-Lucent и является сотрудником лабораторий Bell. Карл работал советником у высокопоставленных членов правительства и лидеров промышленности на пяти континентах, в том числе в качестве вице-председателя подкомитета директоров промышленности Консультативного комитета национальной безопасности по Телекоммуникациям при Президенте США и как руководитель спонсированного Европейской комиссией исследования по доступности и долговечности инфраструктуры электронных коммуникаций. В число последних публикаций входит доклад Института инженеров по электронике и электротехнике «Надежность инфраструктуры подводных кабелей связи в мире». Карл является почетным председателем консультативного совета по Качеству и Надежности связи Института инженеров по электронике и электротехнике, а также основателем и президентом некоммерческой Команды быстрого реагирования по беспроводной связи. Он является изобретателем с более чем 50 зарегистрированными и находящимися на рассмотрении патентами в областях искусственного интеллекта, защиты критически важной инфраструктуры связи, коммуникации в чрезвычайных ситуациях, сохранения энергии, телемедицины. Он лично обнаружил более 1000 программных сетевых ошибок, и неоднократно способствовал распространению рекомендованного экспертами передового опыта.

Валерий Ященко

Валерий Ященко родился 12 февраля 1947 года в Брянской области СССР.

В 1967 году он окончил механико-математический факультет Московского Государственного Университета имени М. В. Ломоносова. В 1971 году окончил в аспирантуру того же факультета.

С 1971 по 1991 год служил на различных должностях в Комитете Государственной Безопасности СССР. В 1991 году ушел в отставку в звании полковника.

С 1991 по 2003 год занимал должность Заместителя начальника лаборатории математических исследований в области криптографии МГУ. В определенный период времени стал советником ректора Московского университета и представляет его в нескольких комитетах Совета Безопасности Российской Федерации.

С 2003 года работает в должности старшего Заместителя директора Института проблем информационной безопасности Московского Государственного Университета имени М.В. Ломоносова.

Имеет докторскую степень по математике (1983).

Эксперты по специальным вопросам

Чарльз (Чак) Барри

Чарльз Барри является старшим научным сотрудником Института национальных стратегических исследований университета Национальной обороны. Отставной военный с обширным оперативным и командным опытом. Доктор Барри более чем 30 лет поводит исследования и публикует работы по трансатлантическим отношениям, военно-политическим вопросам, оперативному управлению и системам управления. Он является членом национального общества почета в области государственного управления и сотрудником Фонда им. Вудро Вильсона. Он получил докторскую степень в области государственного управления (управление информацией) в Университете Балтимора.

Джон С. Эдвардс

Джон С. Эдвардс имеет опыт более чем 51 года работы в сфере телекоммуникаций, в том числе проектировании, анализе и бизнес-планировании. Он успешно создал и управлял несколькими проектировочными группами и основал три компании, одна из которых была позже приобретена крупной корпорацией за миллиард долларов. Доктор Эдвардс занимал должности старшего звена управления в различных компаниях, и в течение 25 лет представлял Nortel Networks в подкомитете директоров промышленности Консультативного комитета национальной безопасности по Телекоммуникациям при Президенте США, где он возглавлял несколько целевых групп. В настоящее время является президентом корпорации Digicom, а также работает в техническом консультативном комитете по информационным системам Министерства торговли США. Он имеет докторскую степень в области электротехники в Университете Пенсильвании.

Дж. Б. (Гиб) Годвин

Контр-адмирал ВМС США (в отставке) Гиб Годвин в настоящее время является вице-президентом по кибербезопасности и системной интеграции в компании Northrop Grumman Information Systems. Используя свой опыт сбора данных и управления системами военной информации, является идейным лидером и новатором в разработке новых подходов к обеспечению

устойчивости киберсистем. Г-н Годвин повышал мастерство сбора данных в течение 15 лет службы в командовании авиационных систем ВМС и командовании боевых космических и морских систем и дослужился до звания контр-адмирала в ВМС США. Там он был исполнительным директором программы информационных систем предприятия, где он обеспечивал взаимодействие ВМС с промышленностью по всем наземным сетевым системам.

Стюарт Голдман

Стюарт Голдман работает в отрасли компьютеров и телекоммуникаций более 45 лет. В этот период он разработал большое количество систем связи и активно участвовал в работе нескольких национальных и международных органов по стандартизации, в том числе в различных руководящих должностях. Он обладает 28 патентами и 50 заявками на рассмотрении. Стюарт является сотрудником лабораторий Bell.

Владимир Иванов

Владимир Иванов является директором московского офиса Института Восток-Запад. До нынешней должности он отвечал за Программу института Восток-Запад по финансовой прозрачности, в том числе публикацию серии исследований по потокам средств между федеральным бюджетом России и регионами. В 2006-2009 годах он играл ведущую роль в сотрудничестве Института Восток-Запад с Россией по развитию международного государственно-частного партнерства в борьбе с терроризмом, особенно в области кибербезопасности, защите критической инфраструктуры и борьбы с незаконной торговлей драгоценными металлами и драгоценными камнями. Владимир в настоящее время принимает участие во всех проектах Института Восток-Запад с участием России, в частности, двустороннем диалоге США и России по вопросам кибербезопасности и евро-атлантической безопасности. Его предыдущий профессиональный опыт включает работу в области социальных наук, деловой журналистики и связей с общественностью. Владимир является автором многочисленных статей по экономике России, опубликованных в газетах Русский Телеграф и Время новостей. Он получил степень бакалавра в области международной журналистики и степень

кандидата исторических наук Московского государственного института международных отношений (МГИМО). Владимир свободно владеет английским и французским языками.

Сергей Комов

Сергей Комов окончил Киевскую высшую школу радиотехники ПВО с дипломом военного радиоинженера. Он получил степень доктора военных наук, профессор, и является автором более 100 научных работ, посвященных информационной войне и информационной безопасности, в том числе обладатель 8 патентов. Принимал участие в разработке Доктрины информационной безопасности России. Он является членом группы экспертов по международной информационной безопасности Министерства обороны России. Он принимал участие в конференции по этой проблеме в формате группы правительственных экспертов ООН (2004-2005), Шанхайской организации сотрудничества (2006-2009), Организации Договора Коллективной Безопасности (2008-2009). Научный советник директора Института проблем информационной безопасности Московского Государственного университета.

Андрей Кульпин

Андрей Кульпин является советником директора Института проблем информационной безопасности Московского государственного университета по международному сотрудничеству. Он также работал и проводил консультации для подразделений Организации Объединенных Наций, в том числе в рамках Целевой группы ООН по борьбе с терроризмом по вопросу противодействия использованию Интернета в террористических целях; работал в экспертной Группе по противодействию терроризму Организации по безопасности и сотрудничеству в Европе; работал по вопросу организованной киберпреступности с Управлением по наркотикам и преступности Организации Объединенных Наций.

Джеймс Брет Майкл

Джеймс Брет Майкл является профессором компьютерных наук и электротехники в Школе повышения квалификации офицерских кадров ВМС США. Он является экспертом по распределенным системам и повышению надежности вычислений. Доктор Майкл является ведущим техническим советником группы экспертов, принимающих участие в разработке Таллиннского Руководства по праву вооруженных конфликтов в киберпространстве. Он является старшим членом Института инженеров электротехники и электроники, имеет награду «Инженер года» общества повышения надежности этого института, имеет степень доктора в области информационных технологий из Университета Джорджа Мейсона.

Пол Николас

Дж. Пол Николас возглавляет команду Глобальной стратегии безопасности и дипломатии корпорации Microsoft, и работает над внедрением стратегических изменений для продвижения безопасности и отказоустойчивости инфраструктуры – как внутри, так и за пределами Microsoft. Он имеет более чем десятилетний опыт решения глобальных проблем, связанных с управлением рисками, реагированием на инциденты, обеспечением связи и обмена информацией в чрезвычайных ситуациях. Г-н Николас занимал пост директора по кибербезопасности и защите важнейших объектов инфраструктуры в Белом доме, помощника директора Главного контрольного управления США, старшего сотрудника Сената, и аналитика Министерства Обороны США. Он получил степень бакалавра в Университете Индианы и степень магистра в Университете Джорджтауна, и является сертифицированным специалистом по безопасности информационных систем.

Джек Ослунд

Джек Ослунд имеет более чем 40 летний опыт работы в правительстве, промышленности и науке в области национальной безопасности и

международных коммуникаций. Он имеет степень доктора наук в области международных исследований в Школе международной службы Американского университета. Он был преподавателем колледжа Национальной военной разведки, входил в Международный секретариат Белого дома по политике телекоммуникаций, и занимал высшие руководящие должности в Корпорации спутниковой связи. Он также участвовал Консультативном комитете по телекоммуникациям по вопросам национальной безопасности, преподавал в качестве адъюнкт-профессора в Университете Джорджа Вашингтона. Он был старшим научным сотрудником Института политики внутренней безопасности Американского университета.

Алексей Сальников

Алексей Сальников является Заместителем директора Института проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова. Его образование включает в себя Технический факультет Высшей школы КГБ, где он специализировался в области математики и криптографии. Его дополнительное образование включает в себя участие в программах Европейского центра исследований по вопросам безопасности Джорджа Маршалла. С 1990 по 2003 год он служил на различных должностях, в том числе Комитете государственной безопасности СССР; Федеральном агентстве правительственной связи и информации (ФАПСИ); и Федеральной службе безопасности (ФСБ). Вышел на пенсию в звании полковника. С 2003 года он был принят на работу в Московский университет. Он является автором более 30 статей и соавтором одной монографии по математическим вопросам криптологии. В настоящее время в круг его интересов входят политические вопросы кибербезопасности, Интернет-мониторинг, криптографические протоколы, и математические проблемы криптографии.

Анатолий Стрельцов

Анатолий Стрельцов является главой отдела Совета безопасности России и полным государственным советником Российской Федерации 3-го класса, полковник (в отставке). Он окончил Ленинградское суворовское военное училище (1964) и Калининскую Артиллерийскую Военную

академию (1969). С 1995 года является сотрудником Совета безопасности России. Имеет ученую степень доктора технических наук (1987), доктора юридических наук (2004), звание профессора (1994), и члена-корреспондента Академии криптографии Российской Федерации (2005). Кроме того, в настоящее время он выступает в качестве советника директора Института проблем информационной безопасности Московского государственного университета.