© Maksymenko E., Zhylin A. The state and personnel policy of the United States of America and the Russian Federation in cybersecurity // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 132-142.

ГОСУДАРСТВЕННАЯ И КАДРОВАЯ ПОЛИТИКА СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ И РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Евгений Максименко, Артём Жилин

Институт специальной связи и защиты информации НТУУ «КПИ», Украина

МАКСИМЕНКО Евгений Васильевич

Год и место рождения: 1973, г. Житомир, Украина.
Образование: Киевский высший военный институт управления и связи им. М.И. Калинина, 1995.
Должность: заместитель заведующего кафедрой.
Научные интересы: компьютерные сети и технологии, численные методы и спектральный анализ, защита информации и информационная безопасность.
Публикации: 4 научных публикации, включая материалы и тезисы докладов на конференциях, статьи в специализированных научных журналах.
E-mail: iszzi@i.ua

ЖИЛИН Артём Викторович, к.т.н.

Год и место рождения: 1982, г. Александрия, Кировоградская область, Украина.
Образование: Житомирский военный институт радиоэлектроники им. С.П. Королева, 2005.
Должность: ведущий научный сотрудник.
Научные интересы: численные методы и алгоритмы факторизации, криптосистемы с открытым ключом, защита информации и информационная безопасность.
Публикации: более 20 научных публикаций, включая материалы и тезисы докладов на конференциях, статьи в специализированных научных журналах.
E-mail: jhartem@i.ua

Аннотация. *Следствием стремительного развития и повсеместного внедрения информационно-телекоммуникационных систем и технологий является зависимость от них практически всех сфер жизни общества: экономической, политической, социальной и др. Последние события в Украине, связанные с аннексией Крыма, проявлениями сепаратизма в Восточных районах и проведением внеочередных президентских выборов являются явным подтверждением «рождения» нового поля ведения противоборства – киберпространства. Для руководства большинства стран вопрос обеспечения безопасности киберпространства стал неотъемлемой частью стабильного и безопасного развития общества и государства. Учитывая сказанное, авторами был проведен анализ открытых документов, отчетов и стандартов в области кибербезопасности. Основное внимание в статье уделено государственной и кадровой политики в области кибербезопасности ведущих мировых держав – США и РФ. В результате анализа были выделены черты, которые присущи как обоим государствам, так и каждому государству отдельно. В качестве выводов также приводится анализ состояния вопросов обеспечения кибербезопасности в Украине.*

Ключевые слова*: кибербезопасность, концепция обеспечения кибербезопасности, Центр академического мастерства в области кибероперацій, учебно-методическое объединение в области информационной безопасности, учебные заведения.*

1. Вступление

Понятия киберпространство, кибер-безопасность и кибератаки все чаще встречаются в нашей повседневной жизни. Сегодня в мире вопросам обеспечения кибербезопасности государства уделяется огромное внимание, что обусловлено объективными процессами развития информационных технологий и их проникновением практически во все сферы человеческой деятельности. Учитывая темпы развития информационных систем, степень зависимости от них буквально всех отраслей экономической, политической и социальной жизней стран, цифровой суверенитет в современном мире становится ключевым элементом независимости государства.

Большинство мировых держав, осознавая важность этого вопроса, уже достаточно давно вносят соответствующие коррективы в государственные политики, отображенные в виде национальных стратегий кибербезопасности или информационной безопасности, где отдельным разделом выделяют кибербезопасность.

Среди основных проблем, возникающих на этом абсолютно новом поле действий можно сформулировать следующие:

- вопросы нормативно-правового характера, связанные с терминологией и законодательной базой: определение киберпространства, как пространства ведения войны, нормативно-правового обеспечения государственной политики в области создания и функционирования подразделений специального назначения;
- вопросы организационного характера: создание, функционирование, взаимодействие, управление и т. д.;
- и, как следствие, достаточно важный вопрос кадрового обеспечения.

В представленной статье не планируется затрагивать вопросы терминологии. Это достаточно проблемная тема и не только для нашего государства. Существенным различиям в подходах к определению понятий, связанных с кибербезопасностью, посвящены отдельные конференции, круглые столы и семинары. Вопросы структуры сил кибернетической безопасности США и других ведущих стран мира, а также предложения к формированию системы подготовки кадров в области кибербезопасности в Украине освещены в [1].

Целью же данной работы является анализ существующих международных документов в области кибербезопасности, а также рассмотрение вопросов организационного и кадрового обеспечения кибернетической безопасности ведущих мировых держав (США и Россия).

2. Актуальность

Анализ вооруженных конфликтов за последние десятилетия (Иран, Сирия, Сомали, Судан и др.) позволяет сделать вывод о том, что их количество и острота из года в год фактически не снижаются. Более того, эти конфликты все чаще охватывают не только традиционные сферы вооруженного противостояния, а именно море, небо и землю, но и постепенно распространяются на новые – информационное и кибернетическое пространство.

В различных источниках описано множество примеров применения кибероружия в современной истории. К числу наиболее ранних вариантов реализации кибератак можно отнести вирус AF/91, внедренный в чип принтера, находящегося на одном из критически-важных объектов (КВО) Ирака. По замыслу разработчиков, во время операции «Буря в пустыне» этот зловредный код должен был вывести из строя систему управления ПВО Ирака.

Достаточно известным является факт проведения американскими спецслужбами диверсионной операции на территории Сербии, в процессе которой была взломана система ПВО страны. В результате данной операции на экранах радаров систем ПВО Сербии отображались десятки ложных целей, что позволило резко уменьшить ее эффективность и провести операцию «Союзная сила» с минимальными потерями.

Также хорошо известен пример незаметного вторжения Израильских ВВС в воздушное пространство Сирии в сентябре 2007 года. Самолеты оставались «невидимыми» для Российских радаров "Игла" и "Панцирь С1Е". Считается, что это было первое боевое использование вирусной программы Suter, разработанной американскими специалистами, задачей которой было выведение из строя систем ПВО противника. Следует отметить, что данный вирусный код впоследствии успешно использовался во время военных конфликтов в Иране и Афганистане.

Последствия внедрения вирусной программы Stuxnet на АСУ ТП атомной электростанции в Иране в 2010 году, в результате которого было выведено из строя оборудование по обогащения урана, оцениваются экспертами в миллионы долларов.

В 2012 году эксперты лаборатории Касперского обнаружили вирусный код Flame, созданный специалистами США и Израиля для ведения кибершпионажа. В июне 2012 года газета Washington Post со ссылкой на неназванных западных чиновников сообщила о том, что шпионский вирус Flame разрабатывался для получения информации, которая могла бы быть полезна для срыва иранской ядерной программы. По данным той же лаборатории в среднем в 2013 году ежедневно обнаруживалось около 315 000 вредоносных объектов, что в 1,5 раза больше, чем 2012 году, при этом за сутки осуществлялось около 4,5 млн. кибератак.

Приведенные примеры подтверждают **актуальность** того, что на современном этапе развития общества кибернетическое пространство все чаще рассматривается в качестве новой арены противоборства, доминирование в которой позволяет сократить потери, как в живой силе, так и в вооружении и технике.

3. Реальный ответ на виртуальное оружие

Большинство мировых держав, осознавая важность и актуальность вопроса обеспечения информационной безопасности, уже достаточно давно вносят соответствующие коррективы в государственные политики. Существует несколько примеров рассмотрения возможности применения вооруженных сил в качестве ответов на кибератаки со стороны других государств. Так после нашумевших в 2007 году Таллиннских событий, связанных с переносом монумента Бронзового солдата и последовавшей за этим крупномасштабной атакой на информационные ресурсы финансовых и государственных структур, власти Эстонии заявили о необходимости приравнять кибератаку к вооруженному нападению. Экс-министр обороны Эстонии Яак Аавиксоо заявил, что предпринятые извне атаки на виртуальное пространство стран-членов НАТО следует приравнять к военному вторжению на территорию этих стран.

В 2010 году группа экспертов НАТО во главе с экс-госсекретарем США Мадлен Олбрайт пришла к заключению, что крупномасштабная кибернетическая атака на командные и контрольные системы альянса или на энергетические сети может привести к ответным коллективным оборонным мерам в

соответствии со статьей 5-й Североатлантического договора [2]. Рассматривался вопрос о том, что даже нет необходимости вносить какие-либо изменения в существующий с 1949 года договор.

16 мая 2011 года на сайте Белого дома был опубликован документ «The U.S. International Strategy for Cyberspace» («Международная стратегия развития киберпространства»). Ключевой особенностью этого документа, который Пентагон подготовил для американского Конгресса, является заявление о возможности применения вооруженных сил в ответ на киберугрозы, источником которых являются сети других стран.

Эксперты назвали этот двенадцатистраничный документ наиболее четким заявлением Вашингтона о политике в области кибербезопасности. В докладе отмечается, что в случае необходимости ответ на атаку в киберпространстве будет таким же, как и на любую другую угрозу в отношении США. При этом правительство США оставляет за собой право использовать все необходимые варианты – дипломатические, информационные, военные и экономические, так как это необходимо для защиты нации, союзников и партнеров, а также интересов государства [3].

Кроме обозначенных документов, затрагивающих вопросы кибербезопасности отдельных государств, существует еще ряд документов обозначающих отношение как международных организаций так и национальных институтов к данной проблеме.

4. Документы, отчеты и стандарты из области кибербезопасности

В 2009 году Международный союз электросвязи (МСЭ) опубликовал отчет «Понимание киберпреступности. Руководство для развивающихся стран» [4], целью которого является содействие развивающимся странам в понимании законодательных аспектов кибербезопасности и помощь в гармонизации законодательных основ.

Руководство содержит исчерпывающий обзор большинства необходимых тем, связанных с законодательными аспектами киберпреступности. В нем описаны проблемы, включая международное взаимодействие и процедуры обмена информацией. Приведены стратегии борьбы с киберпреступниками. Проанализировано международное законодательство, вопросы процессуального характера и т.д.

Следующим знаковым документом, опубликованным в последнее время, является международный стандарт ISO/IEC 27032:2012 «Information technology. Security techniques. Guidelines for cybersecurity» (Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности).

Стандарт дает четкое понимание связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур с точки зрения западных специалистов. Документом определяется, что кибербезопасность и информационная безопасность – это не взаимозаменяемые понятия.

В середине 2013 года Объединенным центром передового опыта по кибероборонe НАТО (Cooperative Cyber Defense Center of Excellence CCD COE) разработан и опубликован документ «The Tallinn Manual on the International Law Applicable to Cyber Warfare», под редакций профессора Майкла Шмидта из Кембриджа [5]. Документ неофициальный, никем не принят и не утвержден. К его разработке были привлечены гражданские и военные юристы из стран НАТО, технические эксперты в области кибербезопасности. Почти на 300 страницах изложены взгляды НАТО на принципы ведения кибервойны, а также с правовой точки зрения дается обоснование действиям членов альянса в киберсреде. Принципы объединены в 95 достаточно подробных правил ведения кибервойны, среди которых есть условия физической атаки на противника и перечисляются условия, при которых гражданские объекты становятся военными и т.д. Разработчики документа считают, что кибератаки по силе воздействия следует приравнять к применению химического, биологического и радиологического оружия. Хотелось бы отдельно отметить, что авторы документа дают понять, что при ведении кибервойн нет нужды в формировании новых законов – достаточно руководствоваться существующими международными правовыми нормами.

Также следует обозначить появление концепций обеспечения кибернетической безопасности как европейских стран, так и мировых державах. При этом существует практика наличия нескольких документов регулирующих разные аспекты кибербезопасности. С существующими национальными стратегиями по кибербезопасности можно ознакомится на сайте Агентства Европейского Союза по сетевой и информационной безопасности (European Union Agency for Network and Information Security) [6]. Описание и анализ всех существующих стратегий и концепций по кибербезопасности не является целью данной статьи. В то же время на фоне проанализированных и обозначенных документов вызывает интерес проведения анализа реализаций государственной политики, в частности кадровой, ведущих стран мира в сфере кибербезопасности.

5. Особенности государственной политики США в сфере кибербезопасности

Начало комплексу мероприятий по защите киберпространства США, проводимых нынешней администрацией Вашингтона, было положено предыдущим главой Америки Джорджем Бушем, который 8 января 2008 года издал директиву по обеспечению национальной безопасности № 54 (National Security Presidential Directive 54 – NSPD-54) и директиву по обеспечению внутренней безопасности № 23 (Homeland Security Presidential Directive 23 – HSPD-23). Именно тогда это начинание бывшего президента и получило наименование The Comprehensive National Cybersecurity Initiative (CNCI

– Комплексная национальная инициатива обеспечения кибернетической безопасности). «Президент Обама определил кибербезопасность в качестве одного из самых серьезных вызовов экономической и национальной безопасности, с которым сталкивается Америка как нация и для борьбы с которым правительство и государство должным образом не подготовлены» [7].

CNCI включает разнообразный комплекс взаимно увязанных направлений деятельности, которые должны обеспечить решение целого ряда масштабных задач, направленных на надежную защиту киберпространства Америки, как в настоящее время, так и в будущем. К ее выполнению привлечены все федеральные ведомства страны, соответствующие органы правительства штатов и структуры местного управления, ответственные за обеспечение защиты киберпространства.

В целом при реализации программ и проектов в обеспечении кибербезопасности США выделено три главные задачи [8]:

- Четкое определение «линии обороны» от атак вероятных противников и создание всех необходимых условий для обеспечения полной информированности специалистов федерального правительства об уязвимости национальных компьютерных сетей, угрозах их безопасности и о ситуациях, складывающихся в ходе функционирования автоматизированных систем, обеспечивающих жизнедеятельность США.

- Обеспечение защиты данных по всему спектру вероятных угроз путем расширения технических и оперативных возможностей контрразведывательных органов США. Кроме того, планируется обеспечить более тщательное закрытие каналов поставок федеральным ведомствам, властным структурам штатов, органам местного управления и частным фирмам ключевых информационных технологий. Это будет сделано для того, чтобы полностью исключить возможность использования этих каналов для незаконного приобретения технических систем и средств противниками Америки.

- Реализация комплекса мероприятий по расширению системы подготовки специалистов по информационной безопасности, повышению эффективности координации финансируемых из федерального бюджета научно-исследовательских и опытно-конструкторских работ (НИОКР) в этой сфере, а также внедрению действенных механизмов их своевременной переориентации, с целью исключения неоправданных расходов на проведение исследований, дублирующих друг друга.

За год до того момента как была опубликована CNCI (2009 год), глава Белого дома утвердил отчет под названием «Обзор политики в киберпространстве» (Cyberspace Policy Review), представленный ему членами специальной комиссии, проводившей анализ состояния дел в области защиты информации, и ее рекомендации по совершенствованию систем охраны киберпространства Америки. Президенту было предложено создать пост координатора по кибербезопасности, который должен регулярно докладывать ему о степени защищенности компьютерных систем США и о мероприятиях, проводимых в этой сфере [9].

В результате в США было создано такое объединение административных структур, которое в состоянии обеспечить организованный и единый поход к противодействию кибератакам на США.

Анализ информации из различных источников только за последний год показывает существенное усиление активности США в сфере кибервооружения. Так по заявлению американского издания «Washington Post», численность сотрудников, которые занимаются обеспечением безопасности правительственных и гражданских компьютерных сетей и систем в США, способных самостоятельно проводить кибератаки, в ближайшее время планируется увеличить более чем в 5 раз до 4,9 тысяч человек.

Согласно информации российского Интернет-ресурса «Военное обозрение», в планы Пентагона входит организация 3-х специальных подразделений: для обеспечения поддержки военных операций, для защиты систем Минобороны и для защиты ключевых гражданских сетей. Данные подразделения получат название «Боевые киберсилы», «Силы киберзащиты» и «Национальные киберсилы».

В дополнение нужно отметить, что по информации различных источников Пентагон собирается создать 30 специализированных команд, которые будут заниматься защитой американских войск, федерального правительства и инфраструктуры страны от киберугроз из-за рубежа. 19 марта 2013 года, на слушаниях в Конгрессе генерал Кит Александер (глава Киберкомандования вооруженных сил США) заявил, что решение о создании таких команд было принято в связи с тем, что информационные системы крупных компаний и госучреждений все чаще становятся объектами компьютерного взлома, а угроза выведения из строя жизненно важных объектов сегодня становится все более реальной и осязаемой. По его словам, предотвратить это можно только при помощи системы активной киберзащиты, которая подразумевает выявление замыслов и планов противника, а также немедленное принятие ответных мер. Александер сравнил это с действиями системы ПРО по уничтожению вражеских баллистических ракет. Именно такой тактики будут придерживаться 13 специализированных команд, на которые была возложена ответственность по обеспечению безопасности киберпространства США. Отдельно отмечается тот факт, что они будут работать не только на территории США, но и за рубежом – то есть, в непосредственной близости от источников потенциальной угрозы, при этом, где именно, генерал не уточнил. Оставшиеся 17 команд будут заниматься защитой баз данных и информационных систем Пентагона, а также американских вооруженных сил.

Кроме всего прочего хотелось бы отметить еще один интересный факт. В настоящее время

рассматривается вопрос о возможности набора в киберподразделения «резервистов» путем создания US Cyber Militia по аналогии с уже существующими в Эстонии Cyber Defence Leage (состоит из программистов и ученых в области компьютерных наук, а также юристов), которые в случае необходимости призываются и переходят в подчинение военным.

Изданные главой Америки директивы по обеспечению безопасности в области кибербезопасности положили начало «кибернетической мобилизации», на фоне которой особо актуальным становится вопрос кадрового обеспечения столь масштабной структуры, выполняющей функции обеспечения кибернетической безопасности США.

6. Кадровая политика США в сфере кибербезопасности

При рассмотрении данного вопроса не планируется обсуждать перечень конкретных учебных заведений, осуществляющих подготовку/переподготовку кадров для подразделений, отвечающих за обеспечение кибернетической безопасности государства. Хотелось бы остановиться на основных подходах и тенденциях в этих вопросах.

В рамках упомянутой ранее «Комплексной национальной инициативы обеспечения кибербезопасности» (Comprehensive National Cybersecurity Initiative), принятой правительством США, было определено, что развертывание специального и общего киберобразования должно стать Национальной стратегией киберобразования по аналогии Национальной стратегии по «модернизации» научного и математического образования в 50-х годах (8 раздел стратегии).

Продолжением выполнения программы «Комплексной национальной инициативы обеспечения кибербезопасности» стала «Президентская национальная инициатива в области киберобразования» (President's National Initiative for Cybersecurity Education), принятая 19 апреля 2010 года. Согласно этой стратегии Агентство Национальной Безопасности (NSA), координирующее вопросы подготовки кадрового обеспечения для киберструктур США, запустило программу CAE-CO (Center of Academic Excellence in Cyber Operations - Центр академического мастерства в области Кибероперацій). По заявлениям официальных лиц NSA данная программа (CAE-CO) направлена на подготовку студентов для работы в U.S. Cyber Command, разведывательных операциях и правоохранительных органах, расследующих киберпреступления. Основной ее целью является сокращение уязвимостей в национальной информационной инфраструктуре путем содействия улучшению качеству высшего образования и научных исследований в сфере кибербезопасности, подготовки большего числа специалистов, которые получали бы практические навыки в рамках различных дисциплин.

Отличительной особенностью Инициативы является четкое определение основных задач и ответственных за их выполнение:

Задача 1: Осведомленность в области национальной кибербезопасности (National Cybersecurity Awareness). Ответственным за решение данного вопроса является Департамент внутренней безопасности (Department of Homeland Security – DHS).

Задача 2: Формализация вопросов киберобразования (Formal Cybersecurity Education) – Управление научно-технической политики Департамента образования (Office of Science and Technology Policy).

Задача 3: Разработка федеральной структуры трудовых ресурсов в области кибербезопасности (Federal Cybersecurity Workforce Structure) – Офис управления кадрами (Office of Personnel Management), который должен провести работы по определению навыков и компетенций для должностей в федеральном правительстве, связанных с вопросами обеспечения кибербезопасности, разработке новых правил для привлечения квалифицированных сотрудников.

Задача 4: Подготовка специалистов по кибербезопасности и повышение квалификации (Cybersecurity Workforce Training and Professional Development) – Министерство обороны (Department of Defense (DoD)), Администрация Директора Национальной разведки (Office of the Director of National Intelligence (ODNI)), Министерство национальной безопасности (Department of Homeland Security (DHS)).

Кроме всего данная Инициатива расширила перечень центров CAE до 181 (на момент дополнения 145), которые позволяют получать соответствующее образование и обеспечивать научные исследования в сфере информационной безопасности под контролем АНБ и Министерства национальной безопасности [10].

Одной из основных задач «Комплексной национальной инициативы обеспечения кибербезопасности» является также выбор учебных (научных) заведений, занимающихся вопросами обеспечения кибербезопасности, в том числе и подготовкой кадров. Данная процедура проводится на конкурсной основе среди учебных (научных) заведений, которые предлагают углубленные технические и междисциплинарные учебные программы, сосредоточенные на таких областях, как информатика, вычислительная техника и электротехника. Учреждения, подавшие заявку должны соответствовать 10 заранее определенным критериям. Анкета для учебных заведений, желающих проводить подготовку специалистов по этой программе, размещена на официальном сайте АНБ [11].

Впервые отбор учебных заведений в рамках анонсированной программы был проведен в 2012 году. Несмотря на то, что заявку на участие в программе подало 20 университетов, лишь 4 было отобрано [12]:

- Государственный университет Дакоты в штате Северная Дакота (Dakota State University);
- Военно-морская школа последипломного образования в Калифорнии (the Naval Postgraduate School);
- Северо-Восточный университет в Бостоне, штат Массачусетс (Northeastern University);
- Университет Талсы в штате Оклахома (University of Tulsa).

Перечисленные учебные заведения получили право осуществлять подготовку специалистов до 2017 года.

Приведем некоторые интересные, на взгляд авторов, факты относительно обозначенных учебных заведений.

Dakota State University (DSU) обладает единственной в своём роде «лабораторий хакинга», где студенты могут научиться тому, как мыслит хакер, какой инструментарий использует, как работает вредоносное ПО, и какими средствами можно противодействовать хакерским атакам [13]. Летом 2014 года на базе DSU будет организован и проведен летний лагерь кибербезопасности. Мероприятие анонсировано как абсолютно бесплатное для посещения и основывается на разработанной в DSU программе Cyber Operations [14].

Одним из ведущих преподавателей Naval Postgraduate School является профессор анализа систем защиты Дороти Дэннинг, занимающаяся исследованиями этических вопросов кибервойны. Среди её студентов есть члены программы обучения Master of Science in Cyber Systems Operations (магистр естественных наук с эксплуатации киберсистем), также как и участники программы Joint Information Operations (совместные информационные операции) [15].

Агнес Чан, заместитель декана и директор последипломного образования (director of graduate education) в Northeastern College of Computer and Information Science, заметила, что NSA были впечатлены моделью «обучения на опыте» (experiential-education) и общим качеством проводимых исследований и образования в области кибербезопасности в Northeastern College [16].

С 2000 года Center for Information Security of University of Tulsa, ныне известный как Institute for information Security или iSec, получил более $25 миллионов из федерального бюджета для своих научных программ. Эти деньги пошли на совершенствование и углубление исследований в различных областях, включая безопасность телекоммуникационных систем, криптографических протоколов, визуализацию сетевых атак, цифровую экспертизу и защиту критической инфраструктуры.

В рамках программы CAE с 2001 года было подготовлено более 250 студентов. Около 90 процентов продолжили работу и профильное обучение в NSA или CIA. Другие выпускники получили работу в DHS, FBI и NASA [17].

В 2013 году АНБ в рамках программы CAE-CO было дополнительно отобрано еще 4 университета:

- Технологический институт ВВС в Огайо (Air Force Institute of Technology in Ohio);
- Университет Оберн, Алабама (Auburn University, Alabama);
- Университет Карнеги-Меллона, Пенсильвания (Carnegie Mellon University, Pennsylvania);
- Университет штата Миссисипи (Mississippi State University).

Среди указанных университетов вызывает интерес Университет штата Миссисипи. Активы университета включают три выделенные исследовательских центра: the Center for Computer Security Research (Центр исследования компьютерной безопасности), the National Forensics Training Center (Национальный тренировочный центр экспертизы компьютерных преступлений) и Critical Infrastructure Protection Center (Центр защиты критической инфраструктуры). Сотрудники и студенты факультетов MSU обладают допусками правительства США к различного рода секретной информации.

Проведение различного рода соревнований так же является одним из традиционных способов подбора квалифицированных кадров в США. Ежегодные учения «Cyber Defense Exercise», проводимые в формате конкурса Агентством национальной безопасности США, направлены на отбор кадров среди обучаемых по гражданским колледжам и военным академиям страны.

Известны и другие подобные соревнования, которые проводят американские организации при поддержки правительства как на территории Штатов так и за их пределами. К их числу относятся, например, Cyber Challenge (международный чемпионат хакеров, который построенный по принципу «захвати флаг»), Киберлагерь в Вирджинии (финал четырехдневных соревнований, организованных программой US Cyber Challenge и Вирджинским политехническим университетом), конкурс Cyber Patriot (общенациональные соревнования для школьников, организованные оборонной корпорацией Northrop Grumman и Ассоциацией военно-воздушных сил).

По результатам анализа вышеизложенного материала можно сделать вывод о том, что Соединенными Штатами Америки уделяется достаточно серьезное внимание вопросам подготовки и подбора кадров для реализации программы обеспечения кибернетической безопасности государства. При этом выбор учебных заведений происходит на конкурсной основе согласно требований, выдвигаемых АНБ.

7. Особенности государственной политики Российской Федерации в сфере кибербезопасности

Что касается России, то здесь не все так просто с понятием «киберберопасность». С одной стороны хотелось бы отметить, что Россия всячески старается обходить использование понятия «кибер-безопасность». В предлагаемой Россией к использованию в рамках ООН «Конвенции об обеспечении международной информационной безопасности» (концепция) предлагается

использовать исключительно термин «международная безопасность».

С другой стороны многие российские чиновники в своих выступлениях постоянно используют слова «киберпреступность», «кибертерроризм», «киберугрозы», но при этом категорически против использования приставки «кибер-« применительно к слову «безопасность».

Одной из первых задач РФ определено продвижение российской «Конвенции об обеспечении международной информационной безопасности» всем государствам – членам ООН. Она носит невоинствующий характер (в отличие от США, рассматривающих киберпространство, как поле военных действий) и направлена на нераспространение кибервооружений и неприменение его в военных и иных целях, направленных против государств.

В отличие от США, Россия не так далеко продвинулась в вопросах создания специальных подразделений, решающих задачи защиты кибернетического пространства, однако предпринято много реальных шагов в вопросах создания законодательной базы. Кроме всего хотелось бы отметить постоянное стремление России ограничить доступ ко всему, что прямо или косвенно касается функционирования всего, что начинается с приставки «спец-». Как уже говорилось ранее, Россия является одним из основных игроков на театре «цифрового противоборства». Прежде всего это благодаря соответствующей политике, проводимой государством, и определением этого вопроса в число наиболее приоритетных.

Так в ходе заседания Совета безопасности в июле 2013 года, целью которого было определение необходимых мер для совершенствования военной организации России на период до 2020 года, президент России В.В. Путин заявил, что к борьбе с сетевыми угрозами необходимо относится, как к одной из наиболее приоритетных задач в оборонной сфере. В свою очередь замглавы российского правительства Дмитрий Рогозин, также присутствовавший на совете, заявил, что средства киберборьбы выходят на первый план. Разрушение связи в войсках с их помощью можно сравнить с артподготовкой.

В ходе визита министра обороны России Сергея Шойгу в Бразилию в октябре 2013 года достигнута договоренность между правительствами двух стран о создании совместной рабочей группы по вопросам кибербезопасности.

Осознание важности вопроса кибербезопасности на современном этапе развития России привело к появлению ряда договоренностей и документов:

1. Министерством обороны подготовлена и опубликована «Концепция деятельности Вооруженных сил в информационном пространстве», описывающая стратегию поведения России в кибернетическом/информационном противоборстве [18].

Концепция представляет собой 14-страничный документ, примерно половина которого отведена терминологическому аппарату. Во всем документе нет упоминания о ведении Россией наступательных боевых действий в международном информационном пространстве. Концепция сводится к трем основным действиям: сдерживанию, предотвращению и разрешению военных конфликтов в цифровом поле.

Интересно заметить, что при этом российские идеологи кибервойны не исключают возможности отвечать на угрозу в виртуальном пространстве методами, принятыми в реальных войнах. Этому посвящен пункт 3.2.5 документа, в котором говорится, что «в условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права».

2. Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». Согласно документу все полномочия по созданию данной системы, разработке методики обнаружения атак, обмену информацией между госорганами об инцидентах ИБ, оценке степени защищенности критической информационной инфраструктуры возложены на Федеральную службу безопасности (ФСБ).

Хотелось бы отметить, что 12.12.2013 Госдума России приняла правительственный закон, который наделяет ФСБ полномочиями по проведению оперативно-розыскных мероприятий для противодействия угрозам информационной безопасности России. Сейчас в рамках оперативно-розыскной деятельности в РФ можно добывать информацию о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности России. Принятый закон к этому списку добавляет информационную безопасность.

3. В настоящее время в Российской Федерации принят ряд документов, направленных на обеспечение различных аспектов национальной информационной безопасности. Среди них Доктрина информационной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации и другие документы. Однако существующее регулирование не охватывает в необходимой мере систему отношений, возникающих в рамках киберпространства как элемента информационного пространства. Поэтому 29 ноября 2013 в Совете Федерации России прошли парламентские слушания, на которых была представлена Концепция стратегии кибербезопасности России [19].

4. В июне 2013 года президенты России и США Владимир Путин и Барак Обама договорились о необходимости создания рабочей группы по вопросам угроз в сфере использования

информационно-коммуникационных технологий. Рабочая группа будет проводить оценку возникающих угроз, разрабатывать, предлагать и координировать конкретные совместные меры по реагированию на такие угрозы.

Главной задачей новоиспеченной структуры является, во-первых, информирование партнера о своей легальной активности в сфере кибербезопасности – чтобы стороны не перепутали учения с агрессией; а во-вторых – обмен информацией о деятельности хакеров, кибер-террористах и специалистах по безопасности недружественных стран. Также предусматривается возможность прямой телефонной связи для общения в случае развития кризисных и экстренных ситуаций.

В средствах массовой информации («Интерфакс», РИА «Новости») последнее время появляется информация о том, что в Вооруженных силах РФ в 2014 (2017 год – Военное обозрение) году будет создано киберкомандование основной задачей которого, будет проведение операций в виртуальном пространстве, как в мирное время, так и в военное. Отмечается, что данное подразделение будет создано как новый род войск.

В феврале 2013 года глава Минобороны Сергей Шойгу потребовал создать детальный план по разработке и внедрению подобного ведомства, призванного защищать российские компьютерные сети и стратегические объекты от угроз, исходящих из виртуального пространства. Планируется, что функции и структура российского кибер-командования будут повторять американский аналог – United States Cyber Command (USCYBERCOM), который вместе с космической и противоракетной обороной подчиняется непосредственно стратегическому командованию.

На встрече с ректорами вузов в МГТУ им. Баумана в марте 2013 года Сергеем Шойгу была выдвинута идея создания в армии научных рот. Ожидается, что в рамках программы студенты-программисты будут выполнять научные работы по заказу Минобороны, которые будут засчитываться учащейся молодежи в качестве прохождения срочной службы в армии.

В отличие от США Россия только начинает формировать как государственную политику в сфере кибербезопасности, так и структуры, которые будут отвечать за ее реализацию. При этом, на ряду с упорным непризнанием некоторыми российскими государственными чиновниками термина «кибербезопасность», в Совете Федерации России уже рассматривается Концепция стратегии кибербезопасности России.

8. Кадровая политика РФ в сфере кибербезопасности

Прежде всего, хотелось бы отметить, что подготовка специалистов в области информацион-но-телекоммуникационных систем определена в число приоритетных направлений модернизации и технологического развития российской экономики. Так распоряжение Правительства РФ от 3 ноября 2011 г. N 1944-р «О перечне направлений подготовки (специальностей) в образовательных учреждениях высшего профессионального образования, специальностей научных работников, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики», определяет перечень около сотни специальностей, в основном технических, связанных с ядерной энергетикой, летательными аппаратами, ракетными двигателями, биотехнологиями, нанотехнологиями, робото-техникой, информационными технологиями и технологиями связи, которые установлены как приоритетные [20].

По состоянию на 2013 год, 74 ВУЗа России занимаются подготовкой специалистов в области информационной безопасности [21]. Для координирования деятельности этих учебных заведений в плане подготовки специалистов, приказом Госкомвуза России от 09.04.96 г. № 613 на базе Института криптографии, связи и информатики Академии ФСБ России (ИКСИ Академии ФСБ России) было создано учебно-методическое объединение вузов РФ по образованию в области информационной безопасности (УМО ИБ).

Основными задачами УМО ИБ являются участие в разработке проектов государственных образовательных стандартов и примерных учебных планов, координация действий научно-педагогической общественности вузов, представителей ведомств, предприятий, учреждений и организаций по обеспечению качества и развития содержания высшего и послевузовского профессионального образования, разработка предложений по структуре отнесенной к его компетенции области высшего и послевузовского профессионального образования и содержанию основных образовательных программ. Так УМО ИБ возглавляет и осуществляет разработку нового профессионального стандарта под названием «Специалист по информационной безопасности», где включена одна из таких областей как компьютерную безопасность. В перспективе на 2014 год спланирована разработка еще 10-15 профессиональных стандартов других областей информационной безопасности.

Разработку указанного стандарта возглавляет Лось Владимир Павлович, д.в.н., профессор, заместитель генерального директора по науке ФГУП «НПП «Гамма», заведующий кафедрой Информационной безопасности МГИУ. Также в разработке стандарта принимают участие специалисты из Федерального государственного унитарного предприятия «Научно-производствен-ное предприятие «Гамма» (ФГУП «НПП «Гамма»), Межрегиональной общественной организации «Ассоциация защиты информации» (АЗИ) и УМО ИБ.

Следует отметить о пленумах и конференциях проводимых в рамках совершенст-вования образования в области информационной безопасности. Так на протяжении 2013 года были

проведены следующие конференции, на которых также затрагивались вопросы по подготовки специалистов в области кибербезопасности.

- 31 мая 2013 г УМО ИБ провело конференцию «Обсуждение проектов Федеральных государственных образовательных стандартов высшего образования по направлению подготовки «Информационная безопасность» уровней бакалавр, магистр».

- 25 сентября 2013 года в Москве в учебном центре Эшелон была проведена конференция «Разработка и принятие профессиональных стандартов – стратегическая реформа кадрового обеспечения. Профессиональный стандарт – Специалист информационной безопасности».

- 30 января 2014 года Национальный форум информационной безопасности «Инфофорум-2014» на тему «Информационная безопасность России в рамках глобального информационного общества». Само мероприятие является ежегодным и проводится в разных регионах как России так и мира.

- 19 февраля 2014 года международный форум по вопросам кибербезопасности «Cyber Security Forum 2014», в котором приняли участие около 1500 российских и международных экспертов.

Кроме академических способов подготовки кадров в рамках образовательных программ ВУЗов, Россия, аналогично США, использует и нестандартные методы подбора специалистов: различного рода конкурсы, олимпиады и киберсоревнования. Ведь ни для кого не секрет, что все эти мероприятия проводятся при активном «кураторстве» силовых ведомств России. К числу наиболее популярных можно отнести различного рода общероссийские или региональные конкурсы RuCTF, VolgaCTF, Defcon CTF, UralCTF, rfCTF, NeoQuest, PHD CTF и т.д., проводимые при активном участии ВУЗов страны.

Отдельно хочется отметить уникальное мероприятие не только в России, но и в мире, которое с 2011 года проводится в Москве: Positive Hack Days. «Только здесь элита хакерского мира, лидеры индустрии безопасности и представители интернет-сообщества встречаются лицом к лицу, чтобы вместе найти ответы на самые актуальные вопросы ИБ» [22]. Тематика PHDays учитывает потребности всего сообщества и поднимает самые актуальные вопросы информационной безопасности: безопасность критически важных информационных систем, противодействие мошенничеству, киберпреступность и расследование инцидентов, государственная и корпоративная безопасность в эпоху WikiLeaks, кибервойна и кибершпионаж и т.д.

Подготовка специалистов в области кибербезопасности в РФ, в отличии от США, основывается на профессиональных стандартах, разработкой которых занимается учебно-методическое объединение вузов РФ под кураторством Академии ФСБ России. Отбор специалистов осуществляется также и во время проведения тематических конкурсов и соревнований.

9. Выводы. Обеспечения кибербезопасности в Украине

Анализ представленной в статье информации позволяет сделать вывод об интенсификации рассмотрения и решения вопросов обеспечения кибернетической безопасности ведущими мировыми государствами. Активные действия на законодательном уровне и в вопросах подготовки специалистов в области кибербезопасности в России и США говорят о важности кибербезопасности в контексте обеспечения национальной безопасности этих держав. При этом следует отметить, что США имеют более основательную законодательную базу в этом вопросе и как следствие уже сформированные подразделения, которые отвечают за кибербезопасность государства. В США подготовка специалистов осуществляется учебными заведениями на конкурсной основе, в РФ же создано УМО, занимающиеся разработкой учебных программ в этой сфере. Как одна, так и другая страна ведет активный поиск специалистов на различных тематических соревнованиях и мероприятиях.

В завершении данного обзора хотелось бы остановиться на проблемах, связанных с обеспечением кибербезопасности в Украине. Анализ Украинского законодательства позволяет сделать вывод, что на данный момент нет ни одного законодательного акта напрямую связанного с понятием кибербезопасности. В течении 2013 года «пытались увидеть свет» несколько документов.

Прежде всего, к их числу относится проект Закона Украины от 07.03.2013 года №2483 «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України», в котором напрямую пытаются отнести вопросы обеспечения кибербезопасности к вопросам обеспечения национальной безопасности государства, связанным с киберпространством.

Следующим документом, определяющим стратегию поведения Украины в цифровом пространстве, является проект Закона Украины від 04.06.2013 р. N 2207а «Про кібернетичну безпеку України» (Автор законодавчої ініціативи: В. Олійник, Ю. Самойленко, О. Кузьмук), в котором кроме определения основных понятий, связанных с киберпространством, определены принципы обеспечения кибернетической безопасности и основные угрозы государства, определены субъекты обеспечения кибербезопасности, их функции и полномочия.

К этому же числу документов можно отнести Проект постановления КМУ «Про визначення порядку віднесення об'єктів до таких, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак», дающий понятие «критически важный объект».

В тоже время, нельзя сказать, что все так плохо. В Украине на основе собственных

возможностей за последние годы также создана соответствующая система подготовки специалистов в области информационной безопасности, к которой можно отнести группу Стандартов Системы Высшего Образования, относящуюся к технической отрасли знаний:

Инженерия (0501 «Інформатика та обчислювальна техніка»; 0502 «Автоматика і управління»; 0508 «Електроніка»; 0509 «Радіотехніка, радіоелектронні апарати та зв'язок»), Естественные науки (0403 «Системні науки та кібернетика»), Безопасность (1701 «Інформаційна безпека»), Международные отношения (0302 «Міжнародні відносини»), Военные науки (1601 «Військові науки, національна безпека»).

Подготовка специалистов по перечисленным направлениям и специализациям проводится в различных государственных, ведомственных и коммерческих учебных заведениях. Можно сказать о том, что на данный момент в Украине не сформирована (или даже полностью отсутствует) законодательная база в сфере кибербезопасности, и как следствие не решены вопросы организационного характера, что негативно влияет на национальную безопасность государства.

Литература

[1] Даник Ю. Г. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України / Ю.Г. Даник, Ю.М. Супрунов// Збірник наукових праць ЖВІ НАУ. – 2011. – Вип. 5. – С. 5-22.

[2] Североатлантический договор [Электронный ресурс]. – http://www.nato.int/cps/ru/natolive/official_texts_17120.htm – Название с экрана.

[3] Международная стратегия кибер-безопасности [Электронный ресурс]. – http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf – Название с экрана.

[4] Понимание киберпреступности: Руководство для развивающихся стран [Электронный ресурс]. – http://www.itu.int/dms_pub/ itu-d/oth/01/0B/D010B0000073301PDFR.pdf – Название с экрана.

[5] Tallinn manual on the international law applicable to cyber warfare [Электронный ресурс]. – http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 – Название с экрана.

[6] National Cyber Security Strategies in the World [Электронный ресурс]. – http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world – Название с экрана.

[7] The Comprehensive National Cybersecurity Initiative [Электронный ресурс]. – http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[8] Лидин А. Киберщит Америки [Электронный ресурс]. – http://vpk-news.ru/articles/6388 – Название с экрана.

[9] 2009 Cyberspace Policy Review [Электронный ресурс]. – http://www.dhs.gov/publication/2009-cyberspace-policy-review – Название с экрана.

[10] Centers of Academic Excellence Institutions [Электронный ресурс]. – http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml#completeList – Название с экрана.

[11] Center of Academic Excellence – Cyber Operations Program [Электронный ресурс]. – http://www.nsa.gov/academia/_files/CAE_Cyber_Ops_Application33_distributed.pdf – Название с экрана.

[12] List of Centers of Academic Excellence for Cyber Operations [Электронный ресурс]. – http://www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_centers.shtml – Название с экрана.

[13] Bachelor of Science in Cyber Operations [Электронный ресурс]. – http://www.dsu.edu/majors-programs/computer-network-security.aspx – Название с экрана.

[14] DSU develops Cyber Security camp for high school students [Электронный ресурс]. – http://www.dsu.edu/news/2013/Cyber-Camp-0827.aspx – Название с экрана.

[15] Kenneth A. Stewart. Cyber Security Hall of Famer Dorothy Denning Discusses the Ethics of Cyber Warfare [Электронный ресурс]. – http://www.nps.edu/About/News/Cyber-Security-Hall-of-Famer-Dorothy-Denning-Discusses-the-Ethics-of-Cyber-Warfare-.html – Название с экрана.

[16] Greg St. Martin. Northeastern designated by the NSA as a National Center of Academic Excellence in Cyber Operations [Электронный ресурс]. – http://www.northeastern.edu/news/2012/05/cyber-operations/ – Название с экрана.

[17] Cyber Corps Program [Электронный ресурс]. – http://www.utulsa.edu/cybercorps – Название с экрана.

[18] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве [Электронный ресурс]. – http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle – Название с экрана.

[19] Концепция стратегии кибербезопасности Российской Федерации [Электронный ресурс]. – http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf – Название с экрана.

[20] Распоряжение Правительства РФ от 3 ноября 2011 г. N 1944-р [Электронный ресурс]. – http://www.garant.ru/products/ipo/prime/doc/55072466/ – Название с экрана.

[21] Учебно-методическое объединение высших учебных заведений России по образованию в области информационной безопасности. Список вузов входящих в состав УМО [Электронный ресурс]. – http://www.isedu.ru/sostav/vuzi.htm – Название с экрана.

[22] Positive Hack Days [Электронный ресурс]. – http://phdays.ru/about/ – Название с экрана.

УДК 004.056:327.5 (045)

Максименко Є.В., Жилін А.В. Державна та кадрова політика Сполучених Штатів Америки й Російської Федерації в області кібербезпеки

Анотація. *Наслідком стрімкого розвитку й повсюдного впровадження інформаційно-телекомунікаційних систем та технологій є залежність від них майже всіх сфер життєдіяльності суспільства: економічної, політичної, соціальної та інших. Останні події в Україні, які пов'язані з анексією Криму, проявами сепаратизму у Східних районах й проведенням позачергових президентських виборів є явним підтвердженням «народження» нового поля ведення протиборства – кіберпростору. Для керівництва більшості країн питання забезпечення безпеки кіберпростору стало невід'ємною частиною стабільного та безпечного розвитку суспільства і держави. Враховуючи сказане, авторами було проведено аналіз відкритих документів, звітів і стандартів в області кібербезпеки. Основну ж увагу в статті приділено державній та кадровій політиці в області кібербезпеки провідних світових держав - США та РФ. У результаті аналізу були виділені риси, які притаманні як обом державам, так і кожній державі окремо. Як висновки також наводиться аналіз стану питань забезпечення кібербезпеки в Україні.*

Ключові слова: *кібербезпека, концепція забезпечення кібербезпеки, Центр академічної майстерності в області кібероперацій, навчально-методичне об'єднання в області інформаційної безпеки, навчальні заклади.*

Maksymenko E., Zhylin A. The state and personnel policy of the United States of America and the Russian Federation in cybersecurity

Abstract. *The result of the rapid development and widespread implementation of information and telecommunication systems and technologies is a dependence on them almost all spheres of life: economic, political, social, etc. Recent events in Ukraine related to the annexation of the Crimea, the manifestations of separatism in the eastern regions and holding early presidential elections are clear evidence of the "birth" of a new field of conducting warfare - cyberspace. For governments of major countries the issue of cyber security has become an integral part of a stable and secure development of society and the state. According to that, the authors analyzed the public documents, reports and standards in the field of cyber security. The main attention is paid to the state and personnel policy in cyber security of leading world powers - the U.S. and Russia. The analysis was highlighted features that are inherent for both states, and that are different. As a conclusion an analysis of the findings in the state of cyber security issues in Ukraine is presented.*

Key words: *cybersecurity, the concept of cybersecurity, the Centre of academic excellence in the field of cyberoperations, teaching union in the field of information security education.*

Отримано *25 березня 2014 року*, затверджено редколегією *29 квітня 2014 року*