Impact Factor:			
ISRA (India) = 1.344	SIS (USA) = 0.912	ICV (Poland) = 6.630
ISI (Dubai, UAE) = 0.829	РИНЦ (Russia) = 0.207	PIF (India) = 1.940
GIF (Australia) = 0.564	ESJI (KZ) = 4.102	IBI (India) = 4.260
JIF = 1.500	SJIF (Morocco) = 2.031	

SOI: 1.1/TAS DOI: 10.15863/TAS

International Scientific Journal

Theoretical & Applied Science

p-ISSN: 2308-4944 (print) **e-ISSN:** 2409-0085 (online)

Year: 2018 **Issue:** 02 **Volume:** 58

Published: 28.02.2018 **http://T-Science.org**

Kamila Famil Jabbarova
doctoral student of the
Institute of Human Rights of
Azerbaijan National Academy of Sciences,
Baku, Azerbaijan Republic.
nauka-xxi@mail.ru

SECTION 22. Policy. Innovations. Theory, practice and methods.

THE IMPORTANT ASPECTS OF STRENGTHENING THE MATERIAL AND TECHNICAL BASE OF THE CYBERSECURITY SYSTEM

Abstract: *The important aspects of strengthening the material and technical base of the cybersecurity system are examined in the article. The problems and the development of space infrastructure of information and communication technologies and the Internet are considered. The necessity of the development of cybersecurity system, the formation of a powerful and a more reliable system to combat cybercrime is substantiated. The effectiveness of cybersecurity system revealed the importance of strengthening its material and technical base are increased with this view. The formation and implementation of modern public policy to improve the rationality of cyber security system and strengthening its material and technical base is argued. The factors and criteria to strengthen the material-technical base of cybersecurity system in terms of the growth of global threats, cybercrime and malicious activities in cyberspace are estimated. The essence of the principles and content of the development and implementation of advanced methods and mechanisms to increase infrastructure, and other structures of the material and technical basis of the system of cybersecurity in the world is revealed. The importance of rationality and deepening innovation and application of innovative features to improve the reliability of the system of cyberspace and cyber countries is particularly underlined. The necessity of constant updating of technological basis, equipment and expanding the list of services in the field of information and communication technologies and the Internet network as a whole in the world of cyberspace is substantiated. The state of security of the material and technical base of cybersecurity system in the world and is priorities for the development and strengthening of material-technical base of cybersecurity system in the current circumstances are estimated.*

Key words: *cybersecurity, cyberspace, material-technical base of cybersecurity system, competitive of control systems cybersecurity, strengthening the capacity of cyberspace and Internet networks, cybersecurity system innovation, state policy of cybersecurity.*

Language: *Russian*

Citation: Jabbarova KF (2018) THE IMPORTANT ASPECTS OF STRENGTHENING THE MATERIAL AND TECHNICAL BASE OF THE CYBERSECURITY SYSTEM. ISJ Theoretical & Applied Science, 02 (58): 154-159.

Soi: http://s-o-i.org/1.1/TAS-02-58-32 ***Doi***: crossref https://dx.doi.org/10.15863/TAS.2018.02.58.32

ВАЖНЫЕ АСПЕКТЫ УКРЕПЛЕНИЯ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

Аннотация: *В статье исследованы важные аспекты укрепления материально-технической базы системы кибербезопасности. Рассмотрены проблемы и развитие пространства инфраструктуры информационно-коммуникационных технологий и Интернет-сети. Обоснована необходимость развития системы кибербезопасности, формирования мощной и более надёжной системы по противодействию киберпреступлениям. С целью повышения эффективности системы кибербезопасности раскрыта важность усиления её материально-технической базы. Аргументированы формирование и осуществление современной государственной политики по повышению рациональности системы кибербезопасности и укрепления его материально-технической базы. Оценены факторы и критерии по усилению материально-технической базы системы кибербезопасности в условиях роста глобальных угроз, киберпреступлений и действий злоумышленников в киберпространстве. Раскрыты сущность принципов и содержание разработки и осуществления прогрессивных методов и механизмов по расширению инфраструктуры, и прочих конструкций материально-технических основ системы кибербезопасности в мире. Особо*

подчёркнуты важность и рациональность углубления инновации и применения инновационных функций по повышению надёжности системы киберпространства и кибербезопасности стран. Обоснована необходимость постоянного обновления технологической основы, оборудования и расширения перечня услуги в сфере информационно-коммуникационных технологий и Интернет-сети, в целом киберпространства в мире. Оценены состояние обеспеченности материально-технической базы системы кибербезопасности в мире и даны приоритетные направления развития и укрепления материально-технической базы системы кибербезопасности в нынешних условиях.

Ключевые слова: *кибербезопасность, киберпространство, материально-техническая база системы кибербезопасности, конкурентоспособность системы управления кибербезопасности, усиление потенциала киберпространства и Интернет-сети, инновация системы кибербезопасности, государственная политика по кибербезопасности.*

Introduction

Проблемы и развитие системы кибербезопасности, создание мощной и надежной системы защиты киберпространства обуславливает формирование и развитие соответствующего ресурсного потенциала и сильной материально-технической базы, сети инфраструктуры, конкурентоспособной системы управления, современной технологии и адекватного механизма по обеспечению кибербезопасности в отдельно взятых странах, так и в целом мире. Одним из главных вопросов обеспечения кибербезопасности является формирование материально-технической базы, которая требует комплексного и системного подхода востребованных огромных финансовых средств и инвестиционных ресурсов. Проблемы создания и развития материально-технической базы системы кибербезопасности, должны найти свое отражение в национальной стратегии по обеспечению кибербезопасности, приоритетных направлениях государственной политики и повседневной деятельности государственных структур, организаций, в том числе частных корпораций и коммерческих организаций в сфере кибербезопасности. Безусловно, вопросы создания и укрепления материально-технической базы системы кибербезопасности обуславливают, как мы отметили, комплексные подходы и в то же время требуется учитывать ряд критерий и принципов по объективной оценке факторов для определения реального создания материально-технического потенциала страны. В первую очередь, необходимо рассмотреть уровень и наличие ресурсного потенциала развития ИКТ и Интернет-сети, их региональных аспектов и финансовой обеспеченности для наращивания дальнейшего пространства развития и укрепления материально-технической базы системы кибербезопасности. Укрепление материально-технической базы системы кибербезопасности способствует повышению эффективности системы защиты киберпространства, бесперебойные работы инфраструктуры ИКТ и Интернет-сети, имеет жизненно важное значение для достижения успеха в обеспечении глобальной безопасности ИКТ и Интернет-сети и открывает возможности обеспечения безопасности информационно-коммуникационных технологий и технологиях, принципах и передовых методах в сфере кибербезопасности в мире. Кроме того, вопросы укрепления материально-технической базы обуславливают активное применение инновационных технологий ИКТ и требуют новые подходы по ускорению инноватизации системы киберпространства и кибербезопасности страны. Новые продукты, технологии, оборудование и услуги в сфере ИКТ и Интернет-сети позволяют создать единую платформу для управления кибербезопасности, рисками и уровнем соответствия нормативным требованиям. Компаниям, коммерческим структурам и государственным организациям на ряду с фешенебельными офисными знаниями, еще необходимы мощные ресурсы, и материально-техническая база в сфере ИКТ и эффективные механизмы, оборудование по борьбе с киберпреступностью, в целом обеспечение кибербезопасности.

Materials and Methods

Вопросы и проблемы реальной оценки состояния материально-технической базы в системе кибербезопасности в отдельных компаниях и коммерческих структурах, в том числе в государственных организациях должны серьезно беспокоить государства стран мира и в первую очередь государства и правительства развивающих стран. Специалисты ИКТ и кибербезопасности департамента политики и стратегии международного союза электросвязи изучали проблемы киберпреступности в развивающихся странах и пришли к выводу, что влияние ИКТ на общество простирается на много дальше, чем создание базовой информационной инфраструктуры. Готовность ИКТ является основой для разработки критерий создания, готовности и использования сетевых услуг [10]. Государству необходимо планомерно и последовательно улучшить материально-технические базы системы кибербезопасности, расширить сеть информатизации, повысить работоспособность и эффективность

инфраструктуры ИКТ и Интернет-сети. Без подобной оптимальной материально-технической базы, системы киберпространства будут подвергаться большим рискам и являться мишенью для хакеров, киберпреступников и прочих злоумышленников виртуально-электронных пространств. А.Макеев считает, что основные аспекты управления рисками информационной безопасности в прямом смысле требуют формирование достаточного материального актива, в том числе вычислительные средства и средства связи и прочие компоненты инфраструктуры информационной безопасности государства [9]. Адекватность и эффективность, в целом оптимальность материально-технической базы системы кибербезопасности при реальной оценке требует учесть, как мы отметили раннее еще и подготовку, повышение квалификации в сфере кибербезопасности. Создавая соответствующие материально-технические базы для развития системы кибербезопасности, параллельно необходимо решить вопросы подготовки специалистов в данной сфере. Дело, в том, что подготовить киберспециалистов не так просто и для этого наряду с определенным временем потребуется большие финансовые средства. М.Бродская справедливо отмечает, что в отличие от многих других областей информационной безопасности, в сфере кибернетической безопасности, критической важных объектов и для качественной подготовки кадров требуется большие инвестиции в создании современных учебно-лабораторных и испытательных диагностических лабораторий [3]. Кроме того, специалисты в сфере кибербезопасности – это есть и интеллектуальные ценности и, исходя из этого вопросы кибербезопасности и интеллектуальное собственность должна рассматриваться во взаимном контексте, которое с развитием глобальной Интернет-среды требует адекватного регулирования отношений с использованием интеллектуальной собственности. Необходимо создать всесторонние возможности и соответствующую среду для развития уровня специалистов в сфере кибербезопасности и их плодотворной деятельности.

Система кибербезопасности является стратегически важным направлением, сферой и одним из главных индикаторов обеспечения национальной безопасности страны. Поэтому государство и правительство стран должны учитывать в ежегодных бюджетах и ассигнованиях достаточную сумму финансовых средств для создания и развития инфраструктуры ИКТ и Интернет-сети и одновременно поощрять частные инвестиции в этих сферах. При оценке уровня надежности материально-технической базы в системе кибербезопасности, особое значение имеет техническая инфраструктура и мощность технических оборудований. Дело в том, что сложные свойства оборудования ИКТ и Интернет-сети требуют постоянное техническое обслуживание и осмотр, профилактические и предупредительные мероприятия. С этой точки зрения необходима сильная и современная техническая инфраструктура и оборудования для обеспечения надежности системы кибербезопасности. Технологические и системные проблемы в основном возникают в результате отсутствия оснащённости и низкого качества технических оборудований инфраструктуры ИКТ и в том числе слабой материально-технической базы. Правительство стран должно уделять особое внимание развитию инфраструктуры, связанной с вопросом обеспечения кибербезопасности страны. Оно должно адекватно оценить важные компоненты и взаимосвязи между прочной материально-технической базой инфраструктуры ИКТ и уровнем обеспечения безопасности киберпространства страны, сделать соответствующие выводы по укреплению мощности материально-технической базы, в целом системы кибербезопасности.

Стоит отметить, что в странах державы развития материально-технической базы киберпространства страны и основные системы кибербезопасности во многом осуществляются военными органами и ведомостями, о чем свидетельствует реальное положение в США и Китае. А.Бобров справедливо отмечает, что в настоящее время пристальное внимание обеспечению своей кибербезопасности уделяют страны НАТО и КНР. Роль лидера в данной области принадлежит США, которая сформировала основы стратегии информационного противоборства еще в 1992 году [2]. С усилением военных ведомостей, разворачивается создание и развитие мощной сети системы кибербезопасности и его соответствующие материально-технические базы, поскольку компьютерные сети и базы данных, ценность информации увеличиваются, они дают возможность повысить степень осведомленности, улучшить взаимодействие между командованиями различного уровня, органами военного управления и разведки, и, тем самым реализовать свои информационные превосходства [8,с.10]. В условиях мобилизованности ресурсы военных ведомостей и прочих специализированных подразделений создают благоприятные условия для создания и развития материально-технической базы системы кибербезопасности, разработки и применения новейших технологий ИКТ и Интернет-сети, обеспечения информационной устойчивости

оборудования и устройств, бесперебойной эксплуатации инфраструктуры ИКТ и основных технических устройств системы кибербезопасности страны.

Как известно, во всем мире растут опасность глобальных элементов национальной угрозы, конфликты, гражданская война и в целом военная опасность, особенно террористическая опасность во всех уголках мира. Все эти факторы и обстоятельства обуславливают развитие инфраструктурной сети системы кибербезопасности, повышение защитной системы и механизмы киберпространства, инфраструктурных объектов ИКТ и Интернет-сети, укрепление национальной системы кибербезопасности стран мира. Кроме того, особо нуждается обеспечение безопасности использование Интернет-сети, которая является наиболее распространенной информационной сетью среди населения, в том числе субъектах всякого рода деятельности, будто ли хозяйственной, коммерческой, социально-экономической, общественно-политической и прочее. Государствам необходимо настойчиво и последовательно заниматься укреплением системы безопасности в инфраструктурах Интернет-сети, повысить мощность материально-технической базы данной сферы, заботиться об их обновлениях, модернизациях и совершенствованиях исходя от характеров и масштаба, глобальных киберугрозов в мире. С.Завьялов отмечает, что в современных условиях Интернет считается наиболее распространённой информационной сетью и поэтому со стороны государства требуется постоянная модернизация и совершенствования программ борьбы с терроризмом, в числе принимаемых мер должна особо уделять внимание на развитие соответствующей материально-технической базы, в том числе средства связи, новые компьютерные технологии и другие инфраструктурные элементы [6]. Отметим, что обеспечение безопасности в сфере информационной технологии и Интернет-сети является приоритетным направлением по выделению ресурсов для развития по тем или иным направлениям инфраструктурного развития системы национальной безопасности, в том числе система кибербезопасности страны. Требуется укрепление не только законодательной базы, принятие соответствующей национальной концепции по обеспечению кибербезопасности страны, но одновременно нуждается к формированию и выделению требуемых финансовых ассигнований на строительстве и в создании прочной материально-технической базы системы кибербезопасности страны. Наряду с укреплением материально-технической базы, требуется уделить серьезное внимание переподготовке и повышению квалификации специалистов в области кибербезопасности и информационной технологии [5]. Или в связи напряжённости по разным факторам в стране требуется одновременное усиление материально-технической и инфраструктурной базы системы кибербезопасности. Например, в связи географическим положением и напряжённой ситуацией на определенных территориях Украины, в том числе продолжение конфликтной ситуации в ряд регионов страны, Украина особо нуждается в укреплении материально-технической базы системы в своей кибербезопасности и предпринимать действенные меры в целом по обеспечению национальной безопасности страны. Правда, в стране в 2016 году была соответствующая национальная концепция по кибербезопасности и мы отметили об этом раннее, однако для укрепления материально-технической базы системы кибербезопасности до требуемого уровня необходимо не малые финансовые средства и новейшие технологии, высококачественные оборудования, которые найти и приобрести для Украины в нынешних условиях не так просто из-за финансовой и экономической нестабильности в самой стране. Президент ICCUkraine Владимир Щелкунов считает, что на Украине отношение к взломам компьютерных систем должно быть таким же серьезным, как и к международному терроризму. Поскольку существует опасность того, что кибератаки могут быть направлены на объекты, критической инфраструктуры [7].

Следует подчеркнуть, что проблемы укрепления материально-технической базы и развитие инфраструктуры киберпространства страны каждым годом становится более актуальной в качестве глобальных проблем для стран мира. Считаем, что подобные проблемы и очень актуально для Азербайджана, которая находится в непростой ситуации, как мы отметили раннее в связи нахождения в условиях войны с Арменией. Как известно, руководство Азербайджана особое значение придает развитию сферы ИКТ и укреплению информационно-электронной безопасности страны. 2013 год был объявлен Годом Информационно-коммуникационных технологий [1]. 13-14 апреля 2015 года в Университете АДА прошла конференция «Национальная безопасность и информационных век», организованная Бакинским проектным координатором ОБСЕ и Министерством иностранных дел Азербайджана. Отмечено, что стремительное экономическое развитие в Азербайджане, сопровождающееся модернизацией инфраструктуры, проникновением информационных технологий в государственной и частном секторе, повышает

необходимость предотвращения киберпреступности в Азербайджане и расширение возможностей борьбы в ней [14].

Conclusion

Все эти факторы и ситуации, связанные с укреплением материально-технической базы системы кибербезопасности должны рассматриваться в контексте самых опасных черт глобальных угроз, национальных интересов и критерий национальной безопасности каждой страны, дабы обеспечить устойчивость и надежность инфраструктуры киберпространства и всей системы кибербезопасности в современном мире. Создание, развитие и укрепление материально-технической базы системы кибербезопасности обуславливают следующее:

- определить оптимальный уровень и источник финансирования системы информатизации и киберпространства, создание соответствующей инфраструктуры ИКТ и Интернет-сети;
- разработать и осуществить комплексные мероприятия развития инфраструктуры ИКТ во всех регионах и пространствах страны, тем самых создать равноправные условия развития системы ИКТ и Интернет-сети во всех уголках страны для расширения потенциала системы кибербезопасности;
- обеспечить комплексные и целенаправленные работы по определению и применению современных технологий ИКТ и Интернет ресурсов, их приложения, оборудование по разным услугам, особенно по обеспечению безопасности киберпространства;
- обеспечить активное взаимовыгодное сотрудничество в сфере ИКТ и ИТ-компаний мира, которые специализировались в той или иной сфере разработки и применения современных технологий в сфере информатизации и обеспечения системы защиты киберпространства;
- расширить деятельность создания соответствующих материально-технических баз ИКТ, таких как инновационные зоны, технопарк по высоким технологиям и оборудованиям, телекоммуникационные и производственные кластеры в сфере информационных технологий и оборудований по системе кибербезопасности;
- обеспечить взаимодействие и кооперационные связи между заинтересованными государственными структурами и частными компаниями по сфере информационных технологий и услуг, расширение перечня услуг ИКТ и Интернет-сети с развитием материально-технической базы;
- обеспечить создание и в дальнейшем развитие современной цифровой инфраструктуры ИКТ и Интернет структуры и соответствующей инфраструктуры по защитной системе киберпространства страны;
- обеспечить систему подготовки и переподготовки кадров, специалистов в сфере ИКТ, Интернет-сети, в целом сфере киберпространства с повышением их квалификации, профессионального уровня;
- обеспечить активное сотрудничество супер державными странами в сфере кибербезопасности и ведущими компаниями мира в области ИКТ и Интернет-сети с привлечением их в сектор ИКТ страны и создать благоприятные условия для поощрения иностранных инвестиций и прихода иностранных инвесторов на этой сфере;
- обеспечить фундаментальное и глубокое изучение опыт создания и укрепления материально-технической базы системы кибербезопасности стран мира, обобщить их и принимать адекватные решения, по их применению исходя из главных задач и стратегических направлений развития системы ИКТ, обеспечения кибербезопасности страны и т.д.

References:

1. Alizade F. (2018) Kiberprostranstvo nuzhdayetsya v zashchite. Available: http://www.zerkalo.az. (Accessed: 10.02.2018).
2. Bobrov A. (2013) Informatsionnaya voyna: ot listovki do tvittera. Zarubezhnoye voyennoye obozreniye, №1, 2013.- p. 23-27.
3. Brodskaya M. (2018) Rossiya stradayet ot defitsita spetsialistov po kiberbezopasnosti. Available: http://www.iecp.ru. (Accessed: 10.02.2018).
4. (2015) V Baku nachala rabota konferentsiya «Natsional'naya bezopasnost' v informatsionnyvek». 13-14 aprelya 2015 .

AzerTAdzh. Available: http://www.1news.az. (Accessed: 10.02.2018).
5. Garifullin S. (2018) Kiberbezopasnost' sverkhu ne spustili. Available: https://www.pnp.ru. (Accessed: 10.02.2018).
6. Zav'yalov S. (2018) Antiterror v Internete: opytstranmira. Available: http://www.sprotyv.info. (Accessed: 10.02.2018).
7. (2018) Zaputalas' v terminakh. Kak Ukrainu zashchishchayut ot kiberugroz. Liga. Biznes. Available: http://www.biz.liga.net. (Accessed: 10.02.2018).
8. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. (2013) Kiberbezopasnost' avtomatizirovannykh system upravleniya voyennogo naznacheniya. Voprosy kiberbezopasnosti, №1, 2013.-p. 10-16.
9. Makeyev A.S. (2016) Osnovnyye aspekty upravleniya riskami informatsionnoy bezopasnosti. Molodoy.uchenyy.- 2016.- № 8.- p. 126-134. Available: http://www.moluch.ru. (Accessed: 10.02.2018).
10. (2009) Ponimaniye kiberprestupnosti: Rukovodstvo dlya razvivayushchikhsya stran. Otdel prilozheniy IKT i kiberbezopasnosti Departament politiki i strategii Sektor razvitiya elektrosvyazi MSE, 2009- 288 p. Available: http://www.itu.unt. (Accessed: 10.02.2018).