http://www.moderntechno.de/index.php/meit/article/view/meit06-01-034
DOI: 10.30890/2567-5273.2018-06-01-034

УДК 004.056

FACTORS OF CONDITIONS OF IMPORTANCE OF CREATING CYBER ARMY OF ARMED FORCES IN DEVELOPING COUNTRIES

ФАКТОРЫ УСЛОВИЙ ВАЖНОСТИ СОЗДАНИЯ КИБЕР АРМИЙ ВООРУЖЕННЫХ СИЛ РАЗВИВАЮЩИХСЯ СТРАН

Hasanov A.H. / Гасанов А.Г.
colonel / полковник
ORCID: 0000-0002-8814-1590
Kerimov E.A. / Керимов Э.А.
d.t.s., prof. / д.т.н., проф.
ORCID: 0000-0002-5957-3044
Military Academy of the Armed Forces, Baku, Sh. Mehtiyev street 136, 107
Военная академия вооруженных сил, Баку, ул. Академика Ш. Мехтиева 136, 1073
Musayeva S.N. / Мусаева С.Н.
c.t.s., as.prof. / к.т.н., доц.
Technical University, Baku, H. Cavid pros. 25, 1073
Технический университет, Баку, пр. Г. Джавида 25, 1073
Hadzhyiev M.M. / Гаджиев М.М.
d.t.s., as.prof. / д.т.н., доц.
ORCID: 0000-0001-7280-3863
Odessa National Academy of Telecommunications O. S. Popova, Str. Kuznyechna 1, 65029
Одесская национальная академия связи им. А.С. Попова, Одесса, ул. Кузнечная 1, 65029
Ivanova L.V. / Иванова Л.В.
c.t.s./ к.т.н.
ORCID: 0000-0003-1738-7697
Odessa Technical College,
Odessa National Academy of Food Technologies, Odessa, Balkivska Str. 54, 65006
Одесский технический колледж
Одесской национальной академии пищевых технологий, Одесса, ул. Балковская 54, 65006

Аннотация. *В статье рассматриваются вопросы защиты военных систем управления, военных технологий, современных оружейных комплексов, систем наведения и других систем от кибер атак и сокращения или предотвращения воздействий кибер атак как, одна из актуальных и неотложных задач национальной безопасности. Проведен анализ разновидностей кибер атак. Приведены статистические данные о вреде, нанесенном кибер атаками в 2018 году разным странам. Проведен анализ опыта развитых стран в вопросах создания национальной системы кибер безопасности.*

Ключевые слова: *кибер безопасность, кибер пространство, кибер армия, кибер атака, хактивизм, кибер защита.*

Вступление.

На современном этапе развития государства кибер безопасность превращается в стратегическую национальную проблему, влияющую на все уровни общества. Гибкая, оперативная и эффективная борьба с кибер угрозами требует правильного определения национальных целей и приоритетов, достигаемых за определенный период времени, а также ролей и ответственности заинтересованных сторон. Национальные стратегии кибер безопасности являются первым шагом в этом направлении.

В среде, где появляются и развиваются все новые кибер угрозы, для стран

имеет большое значение - создание стратегии оперативной кибер безопасности. В современном мире в организации кибер атак по информационным структурам организаций произошли существенные изменения. Эти изменения относятся к целенаправленным и продолжительным атакам Advanced Persistent Threat (APT) [1,2].

Разница APT от традиционных кибер атак заключается в хорошо подготовленном подходном проектировании, планировании, хорошем финансировании и продолжительности действий. Такие типы атак, в зависимости от поставленных задач перед исполнителями, могут продолжаться месяцами, и даже годами. Во многих случаях, целью не становится уничтожение информации или ее искажение, а предполагается получение и анализ информации, и после этого целенаправленное ее использование [3,4].

Термин «Кибер безопасность» в национальной стратегии каждого государства.

Подходы к термину «кибер безопасность» различаются, и в международном уровне нет единого стандарта термина «кибер безопасность» [5,6]. Исходя из этого, проанализируем понятие «кибер безопасность».

По стандартам ISO/IEC 27032 «Кибер безопасность» или «безопасность в кибер пространстве» определяется как обеспечении конфиденциальности, целостности и доступности информации. В свою очередь киберпространство определяется, как единое пространство, не существующее в какой-либо физической форме, но позволяющее создать связи между людьми, программным обеспечением и службами [7].

Из рис. 1 видно, что кибер безопасность не относится к информационной безопасности. Кибер защита тоже в этом статусе, ее назначение – безопасное поведение в киберпространстве, первом делом, защита людей от негативной информации в интернете.

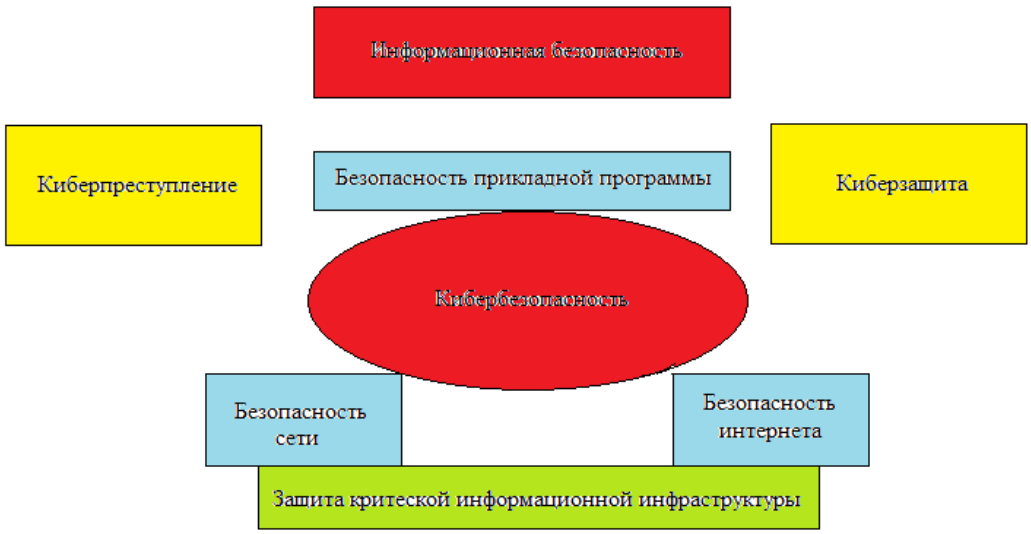

Рис. 1. Отношение между доменами кибер безопасности в кибер пространстве.

В обеспечении кибер пространственной безопасности большую роль играет взаимодействие структур, входящих в кибер пространство. Но, при

очень больших коммуникациях между заинтересованными сторонами в киберпространстве, создаются многочисленные угрозы безопасности. Структуры, которые поддерживают киберпространство и связанные с ним сети, имеют свои интересы. Каждая из структур по своему решает вопросы по эксплуатации и урегулированию общего кибер пространства. Пользователи и провайдеры оценивают обеспечение безопасности с разных точек зрения. Такой фрагментарный подход создает пробелы в безопасности кибер пространства, и для уменьшения таких рисков стандарт ISO/IEC 27032:2012, основываясь на участии заинтересованных сторон, предлагает совместные решения.

Развитие информационно-коммуникационных технологий, наряду с повышением технических возможностей военных систем управления, а особенно автоматизированных систем управления, повысило и угрозы к таким системам. Одним из важных направлений развития военных систем управления в современных условиях является компьютеризация таких отраслей. В итоге, зависимость военных технологий от интернета растет быстрыми темпами - современные оружие, комплексы обнаружения цели и другие системы управляются через интернет [1].

В данный момент развитие всех отраслей управления связано с возрастанием интеллектуальных возможностей интернета и широким использованием информационных ресурсов. В связи с этим, защита современных огневых систем и систем управления против кибер атак является самыми актуальными и неотложными задачами.

Кибер атака.

В современной армии кибер атака и кибер защита считаются неотъемлемой частью всех военных операций. Любая военная операция содержит кибер элементы. Лишь очень немногие армии могут противостоять таким атакам только за счет государственных ресурсов страны.

Кибер атаки делятся на 4 вида: кибер шпионаж, кибер война, хактивизм (от слов хакер и активизм) и кибер преступление [2,3].

Кибер шпионаж - использует обработанные цифровые секретные данные, полученные путем хищения из компьютерных и IT сетей. Например, «Разбор Гаусса» создан для накопления информации и передачи этой информации заказчику [4].

Кибер война - это атака на информацию и информационные системы через интернет. Основной целью кибер войны является: парализовать работу официальных веб сайтов и сетей, привести в негодное состояние системы современного оружия, сервисов, банков, транспорта и др. систем [5].

Хактивизм – это деятельность в направлении нарушения работы интернет сайтов и компьютерных сетей. Хактивисты, применяя этот способ, провозглашают свои политические и общественные идеи [6].

Кибер преступление – как один из видов преступлений совершается с помощью компьютера. Это преступление может исполнятся с помощью различных инструментов и средств кибер атаки [7].

В зависимости от целей и задач, преследуемых кибер атаками в киберпространстве, а также от их потенциала Президентская комиссия по

защите критической инфраструктуры выделила три основных уровня угроз информационной безопасности и относящиеся к ним виды угроз (рис. 2).

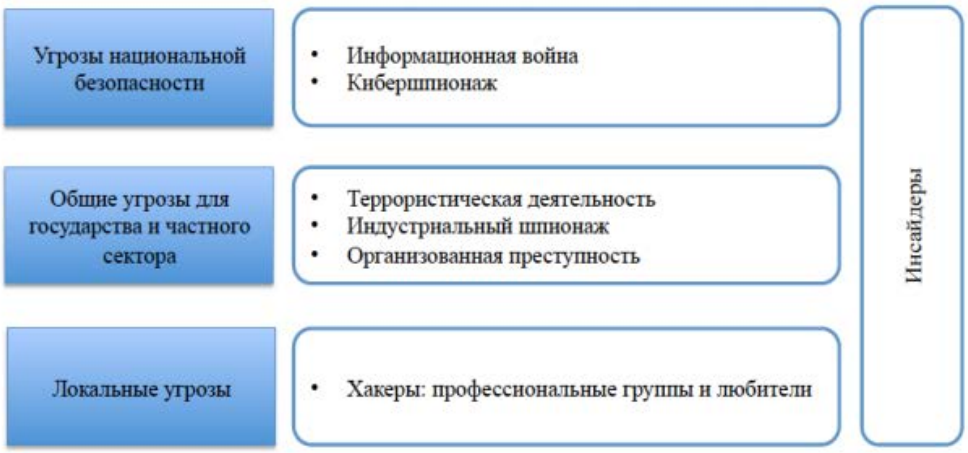

Рис. 2. Уровни угроз информационной безопасности

В настоящее время специалисты отмечают что, III мировая война с большой вероятностью будет кибер войной. Кибер технологии в силе, не производя ни одного выстрела, разрушить системы управления и вооружения.

Чтобы избежать таких ситуаций такие государства как США, Китай, Германия, Израиль, Эстония, Россия, Иран, Грузия и др. сформировали кибер армии. Некоторые страны сделали важные шаги в направлении создания кибер армий, такие как Украина, Иран, Эстония, Грузия и др. страны, которые на себе испытали разрушительную силу кибер преступлений.

На современном этапе развития компьютерные технологии играют важную роль не только в сферах экономики, образования и бизнеса, но и одновременно, для совместного функционирования военизированных систем управления с правительственными организациями. Очевидно, что кибер атаки в современном мире отрицательно влияют на стабильность совместных операций.

По данным “Center for Strategic and Internaional Studies”, в 2017-м году в результате кибер преступлений 10-ти странам (Китай, США, Турция, Россия, Тайвань, Бразилия, Румыния, Индия, Италия, Венгрия) по совокупности нанесен ущерб около триллионов долларов.

Кибер атаки серьёзная проблема для любого государство. Развитые и развивающиеся страны для предотвращения таких атак думают о создании устойчивых систем и создают настоящие кибер вооруженные силы.

Многие страны и корпорации уже начали подготовку высококвалифицированных специалистов в области кибер безопасности. В этом направлении многие корпорации ведут различные работы и вопреки, увеличивающимся с каждым днем кибер угрозам, разрабатываются новые сертификаты безопасности.

Нынешняя ситуация позволяет отметить, что системы управления вооруженными комплексами Вооруженных Сил любых государств должны иметь системы, противостоящие кибер угрозам. Для развивающих стран (постсоветские страны – Украина, Азербайджан, Грузия, Прибалтийские

страны) которые хотят создать электронное правительство, и успешно продвигаются в этом направлении, такие типы кибер атак, и особенно, для Вооруженных Сил таких государств, представляет большую угрозу.

На рис. 3 представлена география кибератак в 2018-м году.

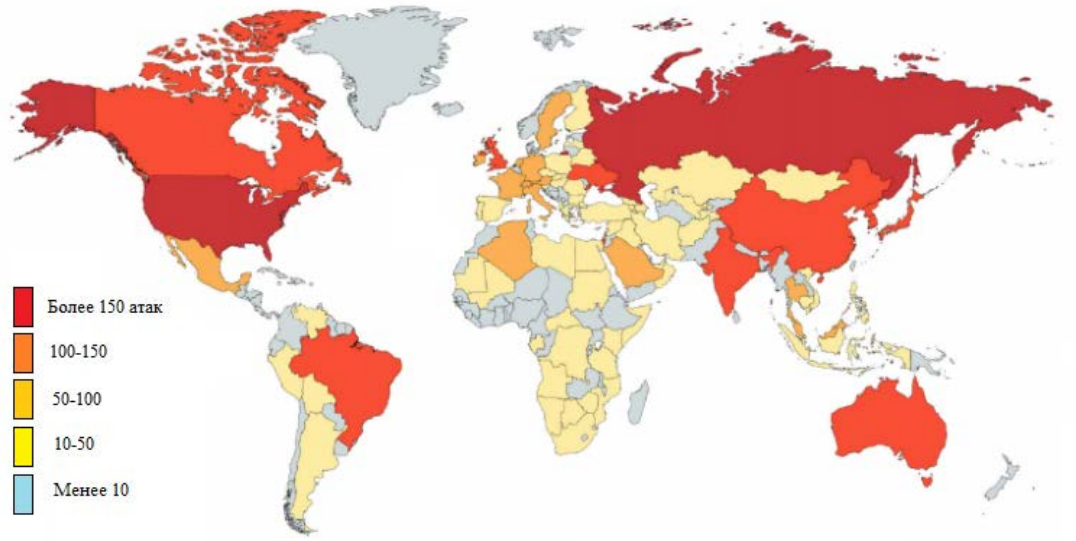

Рис. 3. Исследование кибератак по всей планете в 2017-м году.

Вывод

Основная цель анализа разрушительного действия кибер атак на военизированные системы управления, военные технологии, современное вооружение, комплексы обнаружения цели и другие системы - проявить интерес у ответственных работниках для принятие неотложных мер против действия кибер атак в таких сферах.

Созданная инфраструктура военизированных систем управления на совершенной компьютерной базе включает в себе сложные кибер компоненты. Воздействие кибер атак в таких системах не только разрушительны, но и влекут за собой огромные финансовые потери. С этой целью, развитая безопасная интеграционная модель кибер безопасности должна постоянно усовершенствоваться. Верим, что провиденный анализ для защиты кибер пространство против кибер атак даст возможность для создания национальной системы кибер безопасности и привлечет больше внимания к проблеме кибер безопасности в вооруженных силах в частности.

Литература:

1. Гасанов А.Г. Кибер Безопасность // Военное Знание - Baky, 2014. - № 5. - С. 3-7.

2. Cyber-attacks-statistics, http:// hackmageddon.com /category/ security/ cyber-attacks-statistics, Access time 2018.

3. Cyber-attacks, http://securityaffairs.co/wordpress/12312/cyber-crime/government-networks-totally-vulnerable-to-cyber-attacks.htm l, Access time 2018.

4. Cyber espionage, http://lexicon.ft.com/Term?term=cyber-espionage , Access time, November, 2018.

5. Cyber warfare, http://searchsecurity.techtarget.com/definition/cyberwarfare, Access time, November, 2018.
6. Hacktivism, https://www.techopedia.com/definition/2410/hacktivism , Access time, November, 2018.
7. Cyber-crime https://www.techopedia.com/definition/2387/cybercrime, Access time 2018.

References:

1. Hasanov A.H. (2014). Kiber Bezopasnost [Cyber Security] in Voennoe Znanie [Military Knowledge], issue 5, pp. 3-7
2. Cyber-attacks-statistics, http://hackmageddon.com/category/security/cyber-attacks-statistics/, Access time 2018.
3. Cyber-attacks, http://securityaffairs.co/wordpress/12312/cyber-crime/government-networks-totally-vulnerable-to-cyber-attacks.html, Access time 2018.
4. Cyber espionage, http://lexicon.ft.com/Term?term=cyber-espionage, Access time, November, 2018.
5. Cyber warfare, http://searchsecurity.techtarget.com/ definition/cyberwarfare, Access time, November, 2018.
6. Hacktivism, https://www.techopedia.com/ definition/2410/hacktivism, Access time, Noember, 2018.
7. Cyber-crime https://www.techopedia.com/ definition/ 2387/ cybercrime, Access time 2018.

Abstract. *Protection of military management system, military technologies, modern weapons, aim determining targets and other systems against cyber attacks are studied in the article as one of topical and significant task for preventing influence of cyber attacks. Cyber security is a strategic national problem influencingon all levels of society. On the modern stage of development computer technologies play an important role not only the spheres of economy, education and business but also simultaneously, for the joint functioning of militarized control system with government agencies. In providing cyber of space security a large role is played by co-operation of the structures included in a cyber space. Each of structures on it decides questions on exploitation and settlement general cyber space. Primary purpose of analysis of destructive action cyber attacks on militarized control system, soldiery technologies, modern armament, complexes of finding out an aim and other systems are interest at senior officials for acceptance of urgent measures against an action cyber attacks in such spheres.*

Key words: *cyber security, cyber space, cyber army, cyber attack, hacktivism, cyber defence*

.

Статья отправлена: 21.12.2018 г.