Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 64-74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ANALYSIS OF THE CYBERSECURITY STATUS OF THE INFORMATION SPACE

Nikolay Brailovskyi [1], Valeri Kozura [2], Svetlana Kondakova [3], Volodymyr Khoroshko [2],

Taras Shevchenko National University of Kyiv [1]
National Aviation University [2]
Kyiv National Economic University named after Vadym Hetman [3]

ABSTRACT. The article analyzes the state of the current situation in the information and cyberspace. The differences between cyber influence and cyber threat are indicated and their classification is provided. Issues of cyberterrorism, cyber intelligence and cyberwarfare are considered.

KEYWORDS: information space, cyberspace, cyber influence, cyber threat, cyber terrorism, cyber intelligence, cyberwarfare.

Формирование и развитие современного информационного общества, факт образования которого официально было определенно представителями государств «Большой восьмерки» в ходе Окинавской встречи в июле 2000 года, базируется, как известно [1], на синтезе двух технологий: компьютерной и телекоммуникационной, а также определяется двумя простыми, но очень содержательными законами. Первый закон сформулирован одним из основателей Корпорации Intel Гордоном Муром: «… количество транзисторов в процессорах будет увеличиваться в два раза каждые полтора года…». Этот закон фактически объясняет формирование на рубеже тысячелетий так называемого информационного пространства [1], возникновение новых, специфических по форме и способам, субъектов и объектов информационной инфраструктуры, а также гарантированное возрастание скорости вычислений и объемом информации, которая при этом обрабатывается. Второй закон принадлежит Роберту Меткалфу (изобретателю технологии компьютерной сети Internet), который говорил, что: «…ценность сети находится в квадратичной зависимости от количества узлов, которые есть ее составляющими». Этими словами он констатирует, что основу современного информационного общества составляют сети разнообразного функционального назначения, совокупность и взаимосвязь которых информационное пространство собственно и образовывает [1], а также новейшие информационно-телекоммуникационные (IT) технологии, которые в последнее время:

— стали важной составляющей общественного развития мировой экономики в целом и вместе с тем в значительной степени изменили механизмы функционирования многих общественных институтов и институтов государственной власти;

— вошли в число наиболее существенных факторов, которые влияют на формирование современной высокоорганизованной информационной среды и дают возможность на качественно новом уровне информационного обслуживания в виртуальном и реальном пространствах вести повседневную оперативную работу, осуществлять анализ

состояния и перспективы деятельности информационно-аналитических подразделений, а также добывать исходные данные, необходимые для принятия рациональных научно обоснованных управленческих решений.

Постепенное и довольно условное объединение виртуальных информационно-телекоммуникационных систем (ИТС) и сетевых технологий различного функционального назначения, которые в процессах обработки, передачи и хранения информации используют электромагнитный спектр и действуют как единое целое, а также соответственного программного обеспечения (ПО) привело, как следствие, к формированию так называемого киберпространства - высокоразвитой модели объективной реальности, в которой сведения о личности, предметах, фактах, явлениях и процессах:

— представлены в некотором математическом, символьном или любом другом виде;

— размещаются в памяти любого физического устройства, специально предназначенного для её сохранения обработки и передачи;

— пребывают в постоянном движении в совокупности ИТ систем и сетей.

Под киберпространством разные специалисты в большинстве своём понимают коммуникационную среду, образованную системой связей между объектами инфраструктуры. Учитывая это, наиболее отличительными признаками киберпространства как субстанции является создание и внедрение электронно-цифровых форм обработки, хранения и передачи информации. Кроме этого специалисты считают, что киберпространство имеет непревзойдённые возможности по созданию многочисленных связей между отдельными индивидами и социальными группами с предоставлением разноплановых информационных услуг.

Про важность киберпространства свидетельствует появление концепции ведения борьбы в нём, создание в вооружённых силах ряда стран мира (Россия, США, Китай и другие) специальных структур, предназначенных для ведения такой борьбы – комплекса мер, направленных на осуществление управленческого и/ или деструктивного влияния собственных информационных ресурсов путём использования специальных аппаратно-программных средств.

Такое состояние дел, а также глубокие изменения по отношению большинства стран [2] к собственной информации и, как следствие, кибербезопасности (рис.1) – состояние защищенности киберпространства государства в целом или отдельных объектов инфраструктуры от постороннего влияния, а также своевременного выявления, предотвращение и нейтрализация реальных и потенциальных кибернетических вмешательств, и угроз личным, корпоративным и/или государственным интересам:

во-первых, дают возможность говорить о формировании принципиально новой геостратегической, геоинформационной и геополитической ситуации, когда возникают совсем новые угрозы безопасности для объектов критически важной инфраструктуры этих государств. Получив их, граждане и общество в целом выводят на безусловно более высокий уровень вес исследований, направленных на всестороннее анализ методов, средств, тактики и стратегии действий в информационном и киберпространствах, то есть ведение так называемых информационных и кибернетических воин;

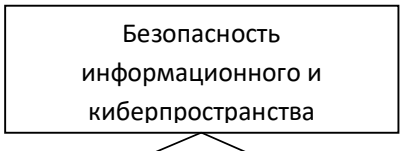

Рис. 1. *Объекты влияния в информационном и киберпространствах*

во-вторых, приводят к беспрецедентному разглашению персональных данных важных корпоративных ресурсов, конфиденциальной информации и информации, которая составляет государственную или другую предусмотренную законом тайну;

в-третьих, обуславливает насчёт кратко и долгосрочных приоритетов трансформации сектора безопасности этих государств по направлениям:

- - поиск и добыча информации путем совершенствования способов и методов организации и проведения атак на ИТ и защищенные криптосистемы противоборствующих сторон и автоматизации всех сопутствующих этому процессов;
- обмен информацией, путем разработки принципиально новых ИТС специального назначения;
- защита собственного информационного ресурса от внутренних и внешних кибервлияний и угроз.

С развитием информационно-коммуникационных технологий (ИКТ), ИТС и глобальные сети интернет мировое сообщество кроме полученных значительных возможностей по обмену информацией стало слишком уязвимым от постороннего кибернетического влияния [1,3], а именно от фактически не прикрытых попыток влияния противоборствующих сторон на информационное и киберпространства друг друга за счёт использования средств в современной вычислительной и/или специальной техники и соответствующего программного обеспечения и других проявлений их дестабилизирующего влияния на определенный объект, которые реализуется за счёт использования технологического и киберпространства, создавая при этом опасность как для их самих, так и для сознания человека в целом.

Инструктивные материалы интернета делят кибервлияние и киберугрозы на такие группы:

- собственно компьютерные инциденты, которые заключаются в вмешательстве в работу вычислительных систем, нарушении авторских прав на программное обеспечение, а также разворовывании данных и компьютерного времени и так далее;

- инциденты, «связанные с компьютерными», которые сопровождаются главным образом противоправными действиями по направлению финансового мошенничества;

- сетевые инциденты, которые способствует осуществлению незаконных договоров.

Существует и другая классификация [3] таких действий. Она определяет 7 основных групп, которые можно отнести к способам или методам, которые используют злоумышленники для совершения нападения, а именно:

- перехват паролей пользователей;
- «социальная инженерия»;
- использование ошибок программного обеспечения и программных закладок;
- использование ошибок механизмов идентификации пользователей;
- использование несовершенства протоколов передачи данных;
- получение информации про пользователей стандартными способами операционных систем;
- блокирование сервисных функций системы, которая атакуется.

Наибольший интерес позиций классификации кибернетических влияний и угроз становится схема, которая предложена конвенцией Совета Европы по борьбе с киберпреступностью. В ней говорится про четыре возможных группы таких действий [1]:

Первая группа — это инциденты, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем, которые реализуются через:

— несанкционированный доступ в информационную среду (противоправный намеренный доступ к компьютерной системе или её части, а также к информационным ресурсам противоборствующей стороны, сделанные в обход системы защиты);

— вмешательство в данные (противоправные изменения, обезвреживание, удаление, перекручивание или блокирование компьютерных данных и управляющих команд, путём проведения кибератак на информационные системы, ресурсы и сети государственного и другого управления);

— вмешательство в работу системы (противоправное нарушение или создание преград функционирование компьютерной системы путем разработки и распространения вирусного программного обеспечения, использование аппаратных и программных закладок, радиоэлектронного и других видов влияния на технические средства и системы телекоммуникации, системы защиты информационных ресурсов, систем и сетей программно-математического обеспечения, протоколы передачи данных, алгоритмы адресации и маршрутизация и так далее);

— незаконный перехват (противоправное умышленное аудирование не предназначенных для общего доступа компьютерных данных, переданных СИТ специального назначения в обход средств защиты и безопасности);

— незаконное использование компьютерного телекоммуникационного оборудование (изготовление, покупка для использования, распространения или другие способы сделать доступными данные: устройства, включая программное обеспечение, разработанные или приспособленные для совершения каждого из преступлений 1 группы: компьютерные пароли, коды доступа, другие подобные данные, которые обеспечивают доступ к компьютерной системе или ее части) или её полное изъятие.

Вторая группа - это мошенничество и подделка, связанные с использованием компьютеров, которые состоят в:

— подделке документов с использованием компьютерных средств (противоправном умышленном внесении, хранении и удалении или блокировании компьютерных данных, которые приводят к снижению достоверности документов);

— мошенничестве с использованием компьютерных средств (вмешательство в функционирование компьютерной системы с целью умышленного противоправного получения экономической выгоды для себя или для других лиц).

Третья группа — инциденты, связанные с размещением в сетях противоправной информации.

Четвёртая группа — инциденты, относительно авторских и смежных прав.

Представленный список не является исчерпывающим, но он даёт возможность [2]:

во-первых, условно объединить приведённые типы действий в 2 укрупнённые категории — вмешательство и угроза, направленные непосредственно на нарушение нормального функционирования ИТС и подключённых к ним компьютеров [1] (тип 1 — по схеме,

предложенной конвенцией Совета Европы), а также традиционные противоправные действия (типы 2, 3, 4 — по той же схеме), которые или связанные с компьютером, или совершены с его помощью;

во-вторых, сделать вывод про то, что определенные таким образом подобные действия в киберпространстве вышли за границы отдельных государств и получили при этом существенную финансовую помощь и качественные коммуникации;

в-третьих, формализовать приведённые типы действий, представив их в виде модели, которая будет содержать 3 главных этапа:

— этап изучения определённого объекта;

— этап проведения нападение на него;

— этап скрытия следов нападения.

Кроме этого, как минимум, в каждом этапе должны быть по 2 стадии — стадия информационного обмена и собственно стадия нападения. Последние, в свою очередь будут состоять из: во-первых, операций по обмену данными, рекогносцировки, отмены и составления карты действий — характерные для информационного обмена и, во-вторых, с операцией получения доступа, расширение полномочий, кражи информации, бомбежки, уничтожение следов, создание «черных ходов» и отказом в обслуживании — характерные для стадии совершения нападения.

Последнее время именно такие действия совершаются противоборствующими сторонами с целью нарушения или блокирования работы информационных систем и сетей в стратегически важных отраслях (объектах) инфраструктуры друг друга, в том числе военного, транспортного, финансового, промышленного и энергетических секторов, а также несанкционированного получения информации из относительно открытых и закрытых баз данных (баз знаний) государственных, коммерческих и других учреждений, их модификации и/или полного уничтожения.

Согласно официальным данным интернета темпы их роста из года в год непременно увеличиваются [4,5]. Это в свою очередь привело к появлению принципиально нового распределения террористических действий в кибернетическом пространстве, который в конце концов получил в СМИ название — кибертероризм [2]. Директор центра защиты национальной инфраструктуры ФБР США Рональд Дик в докладе, который был опубликован на сайте Федерального бюро расследований, так характеризует ситуацию, которая сложилась на сегодня: "... в мире сформировалась новая форма терроризма — кибертерроризм, который использует компьютер и сети связи для разрушения частей национальной инфраструктуры и достижения собственных целей" [1].

Выступая по проблемам мировых угроз, директор ЦРУ Джордж Тенет заявил, что кибертерроризм, распространяясь по миру, может со временем приобрести значительно больших, чем ожидалось, масштабов и, как результат, стать реальной угрозой для национальной безопасности любого государства. По его утверждению, уже угрозы большинства террористических группировок для поддержки своей противоправной деятельности используют последние достижения информационных технологий и компьютерного прогресса — "... компьютерные файлы, электронная почта и криптография и стеганография". Подтверждением этому есть тот факт, что на сегодня в Internet представлены своими файлами абсолютно все известные террористические группы. Они выдают собственные

материалы, как минимум на 40 разных языках и в своей деятельности используют в большинстве такие приемы, как [5]:

— нанесение ущерба отдельным элементам информационного и киберпространства;

— разрушение аппаратных средств, сетей электроснабжения и элементов базы ИТС, а также наведение помех путем использования специальных программ, биологических и химических средств;

— кража или уничтожение информационных, программных и технических ресурсов информационного и киберпространства, которые имеют общественное значение, путем преодоления их системы защиты, внедрения вирусов и разного рода закладок;

— влияние на программное обеспечение и информацию с целью их перекручивания или модификации;

— раскрытие или угроза опубликования, или собственно само опубликование закрытой информации про функционирование информационной инфраструктуры государства, общественно значимые военные информационные системы, коды шифрования и принципы работы шифровальных систем;

— захват канала средств массовой информации с целью распространения дезинформации, слухов, демонстрация силы террористической организации и провозглашение своих требований;

— уничтожение или активное подавление линий связи, искусственные перегрузки узлов коммутации;

— проведение информационных и психологических операций и тому подобное.

Основным способом действия кибертеррористов является проведение атаки на компьютерную информацию, вычислительные системы, аппаратуру передачи данных и другие составляющие ИТ инфраструктуры противоположной стороны.

Это будет способствовать их распространению на систему, которая подвергается атаке, на перехват управления, подавление средств сетевого информационного обмена и совершение других деструктивных влияний.

Кроме отмеченного широко применяется и развивается кибербразведка. Её большинство специалистов по информационно-коммуникационным технологиям (ИКТ) понимает сейчас в основном как самостоятельный метод разведки средствами Internet. На наш взгляд сущность такого вида рода деятельности и основные функции и процедуры на современном этапе развития ИКТ и информационно-телекоммуникационных систем (ИТС) должны заключаться в:

1) систематическом и целенаправленном поиске и сборе информации об объекте разведки с помощью средств ЭВТ и ПО из ресурсов ИТС;

2) изучении, верификации и аналитической обработке накопленной информации, оценке на этой основе возможных угроз (рисков) собственно киберпространства, выявление их признаков и прогнозирование их возможного появления;

3) планирование и, в случае необходимости, осуществление воздействия на киберпространство путем применения активных и/или пассивных методов осуществления противодействия.

То есть, фактически кибербразведка (виртуальная разведка) сейчас представляет собой безусловное сочетание интеллекта, знаний и умений человека, а также внедрение в процесс её деятельности специальных ИТ, направленных на получение банков данных, обеспечение

контроля за сообщениями и информацией, циркулирующих в вычислительных сетях и Internet, получение персональных данных пользователей информационных сетей и другой ценной компьютерной информации.

Следует учитывать, что процесс информатизации всех сторон жизни наполняет качественно новым содержанием разведывательно-информационную работу. Она всё больше сосредотачивается в виртуальном информационном пространстве, заметно меняет роль и место человека в процессе добывания разведывательных сведений и их последующей обработки.

Эксперты спецслужб справедливо делают вывод о том, что складывается особая структура, объединяющая объекты разведки, их информационные образы, запечатлённые в открытом и закрытом информационных массивов, линиях телекоммуникации, выведенных для них, программные и аппаратно-технические средства поиска, преодоление рубежей защиты, обработки полученной информации, ее хранения и распределения [6].

Неотъемлемой частью такой структуры является человек. Эта структура ставит задачи на добычу, поиск, прорыв к защищенному информационному ресурсу, обработки полученных сведений и является потребителем конечной разведывательной продукции, выстраивая на ее основе свою виртуальную действительность, частью которой является сам.

Различные стороны разведывательной деятельности испытывает растущее влияние новых ИТ. Они формируют качественно новые потребности в разведывательно-информационном обеспечении государственной системы принятия политических, военных и экономических решений. Но с такими технологиями открываются и принципиально новые возможности удовлетворения этих потребностей.

Ведущие специалисты по проблемам теории и практики информационной борьбы отмечают, что решающую роль будут играть ИТ — взлом информационных сетей потенциального противника, посещение и уничтожение информации, внедрение дезинформации, внесение компьютерных вирусов и в конечном итоге — полное разрушение системы управления, контроля и выполнения стратегических и тактических планов противника.

Репетициями будущих информационных сражений служат сегодня преступления хакеров, которые вторгаются в информационные сети банков и похищают крупные суммы денег. Для победы в информационном пространстве нужно добиться решающего превосходства над противником в характеристиках и ассортименте суперкомпьютеров, в наборе и содержании программного обеспечения и их возможностях [6,7].

Поэтому, тенденция виртуализации разведывательного процесса отражает закономерный переход к псевдоиерархии узнаваемых природных и искусственных сред — от разведки естественной «первичной», а затем естественной биологической и искусственной среде, возникающей в результате деятельности человека и среды четвертого поколения — искусственного, которая появилась в результате деятельности искусственных интеллектов.

Как считает американский исследователь Майкл Кастанья, сейчас виртуальная (кибернетическая) разведка, которая возникла и совершенствуется — это прообраз разведки будущего. Под понятием "виртуальной (кибернетической) разведкой" — имеется в виду распределенная сетевая организация по производству синтезированной разведывательной информации тактического, оперативного и стратегического уровня с использованием новых ИТ [6].

Исследователи и эксперты обращают внимание на тенденцию, которая всё больше проявляется, виртуализацию деятельности по получению информации. В отличие от традиционной агентурно-оперативной деятельности с целью извлечения разведывательной информации, она ведется преимущественно с использованием новых ИТ в искусственной информационной среде с минимальным участием человека.

Следует отметить и такой важный фактор как кибервойна, которая уже идет. Тема кибервойны в последнее время довольно активно исследуется представителями большинства ведущих стран мира. Пристальное внимание этому вопросу придается также и определенными военными блоками. Так в руководящих документах Североатлантического Альянса кибервойна с недавнего времени рассматривается в одном ряду с противоракетной обороной и борьбой против международного терроризма. При этом в большинстве документов Альянса неоднократно подчеркивается, что из-за роста зависимости стран - членов НАТО от ИТ технологий и увеличения количества атак на их ИТ инфраструктуру, Альянс вполне серьезно подойти к вопросу классификации кибервойны как действия, подпадающего под статью 5 Вашингтонского договора.

Учитывая такое и, несмотря на то, что НАТО уже сегодня имеет три линии кибероборонь, а именно: службу NATO Computer Incidents Response Capabilities Center; Гаагский исследовательский центр проверки действующих систем и выработки новых стандартов защиты и Программу разработки защищенных систем связи, - руководство Альянса в последнее время с целью повышения эффективности ведения военных действий именно в киберпространстве дополнительно разрабатывает [6]:

- специальную структуру для защиты стран-членов от кибератак, которая будет заниматься сбором разведывательных данных и координировать действия членов НАТО в борьбе с киберпреступностью (создание отдельной структуры по предотвращению кибератакам одобрено участниками саммиту НАТО 2-4 апреля 2008 года в Бухаресте. Там же заложено отдельное направление работы альянса под названием "Политика кибернетической обороны");
- концепцию кибервойны будущего, в основу которой положен прежде всего военно-технические концепции C4I (Command, Control, Computer Communication and Intelligence for the Warrior), а также доктрину так называемого киберманевра, что предусматривает разделение всего театра военных действий на две составляющие - традиционную и в киберпространстве (идея предложена в 1996 году экспертом Пентагона Р. Банкер).

В данном случае концепция C4I предусматривает согласованное развитие систем управления, вычислительной техники, связи и разведки. Основным содержанием этой концепции является автоматизация различных процедур сбора, обработки, хранения и передачи информации. В ее рамках планируется достичь высокой степени автоматизации функций целеуказания и распределения информации различного вида, в том числе электронной почты, телеконференцсвязи и т.д. Значительная роль при этом возлагается на внедрение экспертных систем, средств моделирования боевых действий, комплексов технических средств автоматизации, использующих технологии высокопроизводительных ЭВМ и нейрокомпьютеров. Концепция C4IFTW предусматривает, прежде всего, сообщения и функциональную интеграцию систем управления, вычислительной техники, связи и разведки и, во-вторых, создание глобальной информационно-управляющей инфраструктуры, которая

должна обеспечить условия для начала боевых действий крупными военными формированиями без предварительного развертывания систем управления и связи сразу после переброски в места назначения, ее практическую реализацию планируется осуществить за счет: создания совокупности распределенных национальных баз данных, доступных командирам любых уровней; создание устройств сопряжения систем C4I; обеспечение многоуровневой безопасности; жесткой стандартизации требований к сообщениям, процесса испытаний и приобретения систем. Наличие в названии концепций C4I и C4IFTW термина Computer подчеркивает важность того, что применение вычислительной техники среди прочего высокотехнологичным оборудованием в значительной степени изменило способы ведения военных действий и стало жизненно необходимым элементом современных операций. При этом, как подчеркивают военные эксперты, основными объектами поражения на земле и на море, в воздухе и космосе новых войнах будут информационная инфраструктура и психика противника (в связи с этим термин "human network" получает в лексиконе американских военных аналитиков в последнее время все более широкое распространение) [6,7].

Одним из достаточно показательных примеров ведения кибервойны следует считать события 2010 года вокруг сайта Wikileaks на страницах которого была опубликована огромное количество грифованных документов, которые касались войн, которые ведут США в Афганистане и Ираке, а также более 250000 документов переписки американских дипломатов. Специалисты оказались не в состоянии предоставить однозначную оценку этому факту. Часть из них до сих пор считает Wikileaks проектом скрытой операции ЦРУ, что направлена на общую дестабилизацию обстановки в мире. Другие наоборот - характеризуют деятельность сайта как удар собственно по Европе и прямую угрозу западной демократии. Тем не менее, они сходятся в одном - атака, которая была проведена коллективом в несколько десятков сотрудников с годовым финансированием в 200 000 долларов: загрузила разведывательные службы многих стран мира анализом сотен тысяч непроверенных документов; доказала неготовность США - страны, которая имеет огромный арсенал ядерных и обычных вооружений и практически всех ведущих стран мира к ведению кибервойн, их уязвимость для такого рода атак, а также их неспособность обеспечить надлежащий уровень защиты собственных данных; послужила основой для отработки метода давления на некоторых неконтролируемых партнеров путем организованного сбора и обнародования против них ничем не подкрепленных обвинений.

Другим, не менее ярким примером возможности применения новейших ИТ технологий стала также, в последних несколько лет, действия России в киберпространстве.

До последнего времени было не очень понятно, что из себя представляет российская кибервойна. Сейчас картина прояснилась, это многофункциональный инструмент с высочайшим уровнем экспертизы, где задействованы не только тролли, работающие в России, Европе и США, но и огромные группы экспертов, обеспечивающие тончайший анализ актуальных ситуаций и очень быструю реакцию на них. Причём этот анализ и психологический, и политический, и военный.

Кроме того, оказывается воздействие на западные СМИ и институции. Фактически ведется подкуп журналистов и европейских политиков, который измеряется десятками миллионов долларов. И это без учета проектов, конвертированных в пропагандистские инструменты — телевидение, радио, газеты, Internet-издания, а также (что указано в резолюции

Европарламента) большое число институтов, работающих в Европе, США, Израиле и других местах. Плюс индивидуальные соглашения с лоббистами.

Пропагандистские кампании ранее рассматривались как идеологический инструмент для продвижения этих концепций. Первое время так рассматривали и пропагандистскую кампанию в современной России — как продвижение идеи "русского мира". Новое качество состоит в том, что это уже не только продвижение идеологии, но и инструмент ведения войны. Чего стоят только акты вмешательства российских представителей в процессы предвыборных кампаний США, Германии, Украины, Франции и т.д.

Кибератаки и огромные группы троллей только с одной стороны направленные на продвижение идей, а с другой — нацеленный на ведение военных действий, поддержание агентурной сети, деморализация противника, ослабление защитных механизмов и функции государства противника. Сейчас продолжают использовать словосочетание "пропагандистская кампания", хотя речь уже идет об инструментах ведения военных действий, которые наносят ущерб сознанию гражданского населения и вполне могут наносить материальный ущерб.

Таким образом, характерными признаками, которыми сейчас олицетворяют понятие кибербезопасности [2, 3, 4, 6] является совокупность активных защитных и разведывательных действий, которые в процессе информационного противоборства усилиями редких инсайдеров или организованных кибергруппировок разворачивается вокруг ИР, ИКТ, и ИТС [4,7] и которые направлены на достижение и удержание потенциальными противоборствующими сторонами победы в противодействии новым угрозам безопасности для собственных объектов критически важной информационной инфраструктуры.

В последнее время такие действия занимают четкое место в геополитической конкуренции преобладающего большинства стран мира, что в свою очередь обуславливает новые задачи их службам безопасности и вооруженным силам и выводит на первый план проблему информационного противостояния.

Библиография.

1. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки. – К.: Вид. НАУ. 2013 – 432 с.

2. Хорошко В. А. Кибертерроризм и информационная безопасность / Хорошко В. А., Шелест М. Е.// Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні – Вип. 1 (27). 2014. – С.19-14.

3. Козюра В. Д. Методика оцінки рівня безпеки інформаційного простору/ Козюра В. Д., Піскун С. Ж., Хорошко В. О., Хохлачова Ю. Є.// Інформаційна безпека людини, суспільства, держави. №1 (11). 2013. – С. 121-126.

4. Хорошко В. О. Особливості застосування сучасної інформаційної зброї/ Хорошко В. О., Козел Т. І., Ярошенко О. О.// Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 1 (29). 2015. – С.19-15.

5. Гриненко І. Структура кримінальних відносин у кіберпросторі/ Гриненко І., Прокоф’єва-Янчиленко Д., Гончаренко Д.// Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні – Вип. 1 (25). 2013. – С.16-21.

6. Хорошко В.А., Шелест М. Е. Информационно-аналитическое обеспечение безопасности – К.: ВПВ «Задруга», 2016. – 183 с.

7. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки. – Житомир: ЖНАЕУ, 2016. – 636 с.