УДК 004.056.53

ПРИСТАВКА КИБЕР- : ВСЕ ЛИ ОЧЕВИДНО?

Александр Архипов

Рассмотрена сложившаяся на сегодняшний день ситуация, связанная со становлением терминологии в сферах информационной и кибербезопасности. Исследована достаточно давняя проблема подмены термина «безопасность информации» термином «информационная безопасность». Основной акцент в статье сделан на применении терминов с приставкой кибер-. Показано, что с ее помощью выделяется класс киберсистем, используемых для решения задач управленческого характера в самых разных видах деятельности. Однако по сравнению с традиционными системами управления, в которых для осуществления управления реализуется совокупность взаимоувязанных процессов сбора, накопления и обработки информации, в киберсистемах на первое место выдвигается требование непрерывности и устойчивости управления. Это требование может быть выполнено лишь при условии обеспечения доступности, целостности и конфиденциальности исходной информации, привлекаемой для выработки управленческого решения.

В статье анализируются основные свойства современных киберсистем, содержание и взаимосвязь понятий «киберпространство», «кибербезопасность», «киберугроза».

Ключевые слова: *безопасность информации, информационная безопасность, информационное пространство, киберсистема, киберпространство, кибербезопасность, киберугроза.*

Введение

Введенная в действие указом президента П.А.Порошенка в январе 2016 года стратегия кибербезопасности Украины [1] представляет собой базовый документ, позволяющий начать согласованную работу по созданию системы кибербезопасности в Украине. К сожалению, успешному выполнению этой работы явно не будет содействовать отсутствие единой терминологии в сфере информационной / кибернетической безопасности, которое похоже становится уже традиционным. К имеющей место неоднозначной трактовке терминов в информационной сфере [2,3] теперь присоединится неопределенность еще ряда понятий, упоминаемых в стратегии кибербезопасности без каких-либо пояснений или ссылок: ***кибернетическая безопасность, кибернетическое пространство, кибернетическая угроза*** и т.п. Следует отметить, что отсутствие единого нормативно-правового поля в сфере кибербезопасности осознается и авторами стратегии, в частности, в ее четвертом разделе отмечается необходимость разработки отечественной нормативно-правовой и терминологической базы в этой сфере, гармонизации содержания этой базы с другими национальными и международными нормативными документами и стандартами. В предлагаемой статье рассматривается некоторые аспекты этой актуальной проблемы.

Вместо предисловия

Представленный в 1997 году украинский национальный стандарт ДСТУ 3396.2-97 *Защита информации. Термины и определения* стал первым шагом в развитии нормативного обеспечения Украины в сфере защиты информации. Однако из-за незначительного количества вошедших в него терминов этот стандарт был не в состоянии надлежащим образом обеспечить все требования, которые предъявляются к национальной нормативной и методологической базе.

Поэтому вполне логичным и ожидаемым шагом явилось утверждение в апреле 1999 года приказом Департамента специальных телекоммуникационных систем и защиты информации СБУ (ДСТЗИ СБУ) нормативного документа НД ТЗИ 1.1-003-99. *Терминология в области защиты информации в компьютерных системах от несанкционированного доступа*, содержащего список основных терминов в сфере защиты информации (ЗИ), представленных на трех языках (украинском, английском, русском).

Именно в этом документе впервые приводится определение одного из базовых в сфере защиты информации понятий - ***безопасности информации*** (***information security***) – *состояния информации, в котором обеспечивается сохранение определенных политикой безопасности свойств информации* [4]. В этом же глоссарии определяются и соответствующие свойства информации: целостность, доступность, конфиденциальность.

Несколько позже, в 2003 году, утверждается перевод первой части международного стандарта ISO/IEC TR 13335 *Guidelines for the management of the IT security*, получившего в Украине статус национального стандарта ДСТУ ISO/IEC TR 13335 *Інформаційні технології. Настанови з керування безпекою інформаційних технологій*. Используемая в нем терминология, насколько это возможно, гармонизирована с НД ТЗИ 1.1-003-99. Оговорка «насколько это возможно» обусловлена фактами возникнове-

ния некоторых специфических ситуаций: например, используемому в оригинальном англоязычном стандарте эксклюзивному обороту ***система информационных технологий*** по смыслу наиболее близок отечественный термин ***информационная система*** (ИС). Можно утверждать, что в целом к этому моменту в Украине сложилась достаточно полная и непротиворечивая система понятий в области безопасности информации. В новой семействе международных стандартов серии ISO/IEC27XX, появившейся после 2000 года, трактовка основных терминов практически не изменилась. В частности, в последней (четвертой) редакции стандарта-справочника ISO/IEC 27000:2016. *Information technology. Security techniques. Information security management systems. Overview and vocabulary* в разделе 2 дается следующее определение: ***безопасность информации*** (***information security***) – *сохранение конфиденциальности, целостности и доступности информации.*

Описанная выше ситуация с использованием термина ***безопасность информации*** на первый взгляд выглядит вполне благополучной. Тем не менее это не совсем так.

Начиная с конца 89-х - начала 90-х годов прошлого века в публикациях, посвященных анализу и исследованию проблем глобальной информатизации общества, широкое распространение получил термин ***информационная безопасность***. Свое нормативное определение он обрел значительно позже – в 2007 году. Закон Украины *Об основных принципах развития информационного общества в Украине на 2007 - 2015 годы* определяет ***информационную безопасность*** *как состояние защищенности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесение вреда через: неполноту, несвоевременность и недостоверность используемой информации; негативное информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации.*

Очевидно, что понятие ***информационная безопасность*** по своему объему несравненно шире объема понятия ***безопасность информации***, включая в себя последнее в том контексте, что нарушение ***безопасности информации*** – лишь одна из ряда возможных причин, ведущих к нарушению ***информационной безопасности***. При этом для ***информационной безопасности*** объектом защиты является личность, общество (или его отдельные социальные группы), государство, тогда как в ***безопасности информации*** объект защиты – исключительно информация.

Тем не менее, несмотря на столь существенное смысловое различие, к концу 90-х годов прошлого века значительная часть специалистов, по характеру своей деятельности принадлежащих к сфере обеспечения безопасности информации, тематику своих работ упорно относит к другой сфере - сфере информационной безопасности. Причин этому несколько.

В первую очередь следует заметить, что практически все русскоязычные переводы международных стандартов, касающихся вопросов безопасности информационных технологий, при наличии в них раздела <Термины и определения> дают нам формулировку такого содержания: ***информационная безопасность*** (***information security***) – *защита конфиденциальности, целостности и доступности информации* [5]. Происходящая очевидная подмена понятий, обусловленная некорректным переводом с английского языка на русский термина ***information security***, и отмечаемая рядом авторов [2; 3; 6], тем не менее уверенно закрепляется в нормативных документах, в первую очередь в переводных международных стандартах [7; 8].

К сожалению, аналогичная ситуация сложилась и с украиноязычным переводом стандарта ISO/IEC 27001, получившим статус отраслевого стандарта ГСТУ СУІБ 1.0/ISO/IEC 27001:2010, в оригинале которого имеем: ***інформаційна безпека*** (***information security***) - *збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність*, хотя фактически дается определение термина ***безопасность информации*** – сохранение конфиденциальности, целостности. При этом следует учитывать, что к моменту выполнения перевода в отечественном нормативно-правовом поле уже существовали определения обоих понятий, т.е. авторы перевода проигнорировали и отечественную нормативно-правовую базу, и сложившуюся в процессе перевода стандарта ISO/IEC TR 13335 традицию перевода.

Второй причиной приоритетного использования понятия ***информационная безопасность*** в какой-то мере может служить уже упомянутый выше факт поглощения этим понятием более узкого понятия ***безопасность информации***, хотя по-видимому основная причина сложившейся ситуации состоит в том, что отечественные специа-

листы изучение нормативно-правовой базы начинают со знакомства с некачественными и часто неавторизованными переводами зарубежных стандартов, в изобилии представленных в Интернете.

В связи с вышеизложенным интерес вызывает набирающий темп процесс формирования терминологии в сфере кибербезопасности, в частности, определение самого понятия ***кибербезопасность***.

Приставка кибер- – все ли понятно?

Действующий ныне стандарт ISO/IEC 27032 [9] содержит следующее определение: ***кибербезопасность***, ***безопасность киберпространства*** (***cybersecurity***, ***cyberspace security***) - *сохранение конфиденциальности, целостности и доступности информации в киберпространстве*. Это определение, учитывая приведенные выше дефиниции терминов, можно трансформировать в более краткую форму: ***безопасность киберпространства*** - ***безопасность информации*** *в киберпространстве*.

Смысл обоих формулировок становится частично понятным, если предположить, что объемы киберпространства и информационного пространства не совпадают, например, киберпространству соответствует только некоторая ограниченная область более обширного информационного пространства. При этом общий объем всей информации, циркулирующей в информационном пространстве, очевидно будет больше объема информации, циркулирующей только в киберпространстве, но именно *сохранение конфиденциальности, целостности и доступности информации* в этом меньшем объеме и определяется термином ***безопасность киберпространства.***

Однако это незначительное и чисто формальное замечание никак не касается основного проблемного аспекта предложенных выше формулировок: в них используются термины ***информационное пространство*** и ***киберпространство***, не определенные в украинском нормативно-правовом поле и, следовательно, требующие отдельного уточнения.

В отечественных публикациях термин ***информационное пространство*** появился в начале 90-х годов прошлого века***,*** *определяя некую системную сущность, структурными компонентами которой являются информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура*. В предисловии к словарю-справочнику [10] ***информационное пространство*** - *среда, в которой осуществляются процессы создания, сбора, регистрации, обработки, накопления, сбережения, поиска, защиты, распространения и использования информации*… ". Одно из официально принятых определений (Решение экономического совета СНГ "О концепции научно-информационного обеспечения программ и проектов государств-участников СНГ в инновационной сфере"): ***информационное пространство*** - *совокупность баз и банков данных, информационно-телекоммуникационных сетей и систем, а также технологий их ведения и использования, функционирующих на основе общих принципов и по правилам, обеспечивающим информационное взаимодействие организаций и граждан...*"

Термин ***киберпространство***, также, как и другие термины с приставкой ***кибер-*** в сфере безопасности, появился относительно недавно. Уже упоминавшийся ранее стандарт ISO/IEC 27032 [9] трактует киберпространство *как сложную среду, возникающую в результате взаимодействия людей, программного обеспечения и интернет-услуг с использованием средств телекоммуникаций и сетевых технологий*. В этой формулировке замена ***киберпространства*** на ***информационное*** дает дефиницию, весьма близкую последнему определению термина ***информационное пространство***, т.е. в интерпретации стандарта ISO/IEC 27032 ***киберпространство*** практически совпадает с ***информационным***.

Еще более парадоксально определение, приведенное в [11]: ***киберпространство*** - *это среда, которая возникает в результате функционирования на основе единых принципов и по общим правилам информационных, телекоммуникационных и информационно-телекоммуникационных систем*. По всей видимости, совокупность функционирующих по единым принципам и общим правилам информационных систем, соединенных между собой средствами телекоммуникаций, должна порождать ***информационное пространство***, но при чем здесь ***кибер-***?

Таким образом, из анализа приведенных выше формулировок терминов ***киберпространство*** и информационное ***пространство*** следует два вывода: либо данные формулировки не содержат необходимых сведений, обеспечивающих надежную дифференциацию этих терминов, либо понятия ***безопасность киберпространства и*** безопасность ***информации*** совпадают.

В контексте этого замечания интерес представляет несколько метафорическое определение [12]: ***информационное пространство*** – *форма существования информационных систем*, своеобразной калькой которого будет определение ***киберпространство*** – *форма существования кибернетических систем*. Очевидно, что ключевым моментом, позволяющим выявить различие этих двух формулировок, является определение понятия ***кибернетиче-***

ская система (***киберсистема***), в частности, интерпретация семантических особенностей приставки ***кибер-***.

Прилагательное ***кибернетическая*** (сокращенно - ***кибер-***) производно от термина ***кибернетика*** - *наука об управлении, получении, передаче и преобразовании информации в* ***кибернетических системах*** [13]. Исходным понятием ***кибернетики*** является управление, представляющее собой результат выполнения целенаправленной упорядоченной последовательности преобразований информации, реализуемых в ***кибернетической системе***. При этом под ***кибернетической системой*** понимается *совокупность связанных друг с другом элементов, способных воспринимать, хранить, перерабатывать информацию, а также обмениваться информацией* [13]. В общем случае ***кибернетическая система*** представляется в виде контура информационных обменов, состоящего из управляемого объекта, управляющей системы, датчиков исходной информации и каналов передачи информации. Информационно-транспортный сегмент ***кибернетической системы*** представлен процессами, обеспечивающими поступление в управляющую систему необходимой информации (процессы восприятия исходной информации, ее передачи, получения, хранения), а собственно управление осуществляется путем преобразования (переработки) поступившей исходной информации в сигнал (информацию) управления, корректирующий состояние управляемого объекта. Таким образом, структурно любая киберсистема – совокупность элементов, реализующих набор информационных технологий, сохраняющая базовые признаки и свойства информационной системы. Поэтому попытка различения информационной и киберсистемы путем задания соответствующих дефиниций, основывающихся на результатах обобщенного структурного анализа каждой из этих систем, обречена на неудачу, что и наблюдается выше.

Эффективным является введение в дефиниции сведений о функциональном предназначении соответствующих систем, например: ***кибернетическая система*** - *информационная система, предназначенная для выполнения функции управления* (*принятия решения*) *в разных сферах деятельности*.

В этом случае справедлива следующая схема:

- информационные системы – **род**, допускающий сегментацию на **виды**, один из которых составляют информационные управленческие системы;
- ***кибернетические системы***, в свою очередь включающие ряд **подвидов**.

Например, к ***кибернетическим системам***, в зависимости от принятой системы классификации, обычно имеющей национальные особенности (в частности, отражающиеся в наименованиях), можно отнести: АСУ ТП, АСУ П, SCADA – Supervisory Control and Data Acquisition, CNC – Computer Numerical Control, SCM – Supply Chain Management, CRM – Customer Requirement Management и т.д.

Характерный пример формирования терминов с приставкой ***кибер-*** дает практика употребления официальных наименований подразделений в вооруженных силах США. В ноябре 2006 г. в США было создано кибернетическое командование военно-воздушных сил - AFCYBER (сокращение. от англ. Air Force Cyber Command), на базе которого с привлечением других подразделений, в 2009 г. формируется кибернетическое командование США (англ. United States Cyber Command, USCYBERCOM), задачей которого является обеспечение устойчивого и непрерывного управления войсками, стабильной информационной поддержки, в частности, устойчивого взаимообмена информацией, и защита соответствующей информационной инфраструктуры, что является необходимым условием устойчивости и непрерывности управления [14; 15]. Как видим, для киберподразделений, в дополнение к «классическим» процессам управления, обмена и переработки информации, добавляется функция обеспечения устойчивой реализации этих процессов, выполнение которой гарантируется мерами по поддержанию необходимого уровня безопасности информации. По-видимому, именно это последнее свойство становится отличительной особенностью современных киберсистем, а выполнение требования по обеспечению доступности, целостности и конфиденциальности исходной информации, привлекаемой для выработки управленческого решения в киберсистемах, определяет содержание понятия кибербезопасность.

Очевидно, что киберсистемам, как сегменту информационных систем, соответствует некоторая ограниченная область полного ***информационного пространства***, которая и представляет ***киберпространство***, в пределах которого определено понятие ***безопасность киберпространства***. Из рассмотренных выше материалов, касающихся сферами безопасности информации и кибербезопасности, очевидно, что ***безопасность киберпространства*** (***кибербезопасность***) образуется сужением более общего понятия ***безопасность информации***.

Что касается понятия ***кибернетическая угроза*** (***киберугроза***), то к таковой может быть

отнесена любая угроза информации в ***киберпространстве***. Тем не менее, в ряде случаев с ***киберугрозами*** связывают угрозы, возможность реализации которых рассматривается по отношению к объектам критически важной инфраструктуры (иначе - критически важным объектам (КВО)) [1], т.е. к объектам, нарушение или прекращение функционирования, которых ведет к катастрофическим последствиям для страны и населения в целом либо для ее отдельных административно-территориальных единиц. Однако сами по себе большие потери не являются достаточным признаком существования киберугроз. Например, ошибки, возникшие из-за использования неточных исходных данных при проектировании плотин, несущих конструкций или силовых элементов КВО, могут повлечь возможные катастрофические последствия, которые, однако, не будут иметь отношения к киберугрозам. Определяющим признаком в диагностировании киберугроз относительно критически важных объектов энергетики, промышленности, транспорта, связи, госуправления т. п., является реализация информационных угроз относительно кибернетических систем, осуществляющих функции управления соответствующими КВО (в частности, автоматизированных систем управления (АСУ) на производстве, в военной и других сферах деятельности). При этом, когда речь идет об осуществлении киберугроз в КВО транспорта, связи, химической промышленности, ядерной энергетики и пр., реальные потери могут быть чрезвычайно высоки.

Рассмотрим еще один нюанс, связанный с употреблением термина ***киберпространство. Информационное пространство*** – это множество разнообразных динамично взаимодействующих информационных потоков и полей, генерируемых информационными системами (ИС) и телекоммуникационными системами (ТКС), обеспечивающими потребителя нужными ему информационными продуктами и услугами. Значительное внимание при эксплуатации современных информационно-телекоммуникационных систем (ИТС) уделяется вопросам защиты информации. Эффективность и результативность решения этих вопросов обеспечивается функционированием системы менеджмента защиты информации [16], поэтому с позиций кибернетики комплексная система защиты информации относится к кибернетическим системам. В идеальной системе защиты информации должен обеспечиваться контроль всех возможных информационных потоков в защищаемом объекте (концепция диспетчера доступа [17]), т.е. фактически всего ***информационного пространства*** объекта защиты. Следовательно, если ***информационное пространство*** для данного территориального сегмента порождено совокупностью защищенных ИС, ИКС, ИТС, то ***киберпространство***, порождаемое функционированием соответствующих систем защиты, будет совпадать с ***информационным пространством***.

Для большинства современных ИС, ИКС, ИТС обязательно наличие система защиты информации. Поэтому во многих случаях использование компьютеров в организации уже является достаточным основанием для применения в отношении ее информационных систем терминов ***киберпространство***, ***безопасность киберпространства***, ***киберугроза.*** В частности, согласно терминологии США, ***киберпространство –*** это глобальная информационная сфера, состоящая из взаимозависимых инфраструктур информационных систем (включая интернет), телекоммуникационных сетей, компьютерных систем, встраиваемых процессоров и контроллеров [27002], при этом вместо практически не используемого термина ***безопасность информации*** повсеместно применяется термин ***кибербезопасность***.

В заключение отметим, что в некоторых определениях понятия ***киберпространство***, например, в приведенном выше определении из стандарта ISO/IEC 27032 [9], среди обязательных составляющих, обеспечивающих порождение киберпространства, упоминаются люди. В данной статье это -специалисты-профессионалы (операторы, эксперты, лица, принимающие решения и пр., входящие в состав персонала информационных и кибернетических систем, владельцы или собственники информационных ресурсов, элементов инфраструктуры, пользователи и потребители информационных ресурсов и услуг), чья деятельность связана только с вопросами безопасности информации и не касается аспектов манипулирования массовым или индивидуальным сознанием. Эти, несомненно важные и актуальные аспекты, относящиеся к управлению в социальных системах, выходят за рамки декларируемых в стандарте ISO/IEC 27032 задач сохранения конфиденциальности, целостности, доступности информации в киберпространстве, и принадлежат к компетенции информационной безопасности.

Выводы

1. Обеспечение решения управленческих задач для различных видов деятельности составляет цель функционирования кибернетических систем (киберсистем). Защите в киберсистемах подлежит специфический вид информации – управленческая информация, т. е. информация, используемая

для выработки управленческих решений. Незащищенность этой информации может повлечь ухудшение качества управления вплоть до наступления катастрофических последствий, как для объекта управления, так и для его окружения, в частности персонала и населения. Для современных киберсистем, в особенности систем управления критически важными объектами, задача обеспечения качества управления, и в первую очередь его устойчивости и непрерывности, становится первоочередной.

2. Кибербезопасность, безопасность киберпространства (cybersecurity, cyberspace security) - сохранение, целостности, конфиденциальности и доступности информации, циркулирующей в киберсистеме (т. е. поступающей в киберсистему, накапливаемой и хранимой в ней для последующей обработки) с целью обеспечения устойчивости и непрерывности реализации киберсистемой управленческих функций относительно соответствующих объектов управления.

3. Киберпространство – пространство, образованное информационными потоками и информационными полями, порождаемыми в процессе функционирования кибернетических систем.

4. Для ИС, ИТС, безопасность информации в которых обеспечивается функционированием систем менеджмента защиты информации (являющихся подвидом кибернетических систем), киберпространство, порождаемое функционированием систем защиты, практически совпадает с информационным пространством соответствующих ИС, ИТС.

ЛИТЕРАТУРА

[1]. Стратегія національної безпеки України. Указ президента України №287/2015 від 25.05. 2015 р. [Електронний ресурс] – Режим доступу: http://zakon5.rada.gov.ua/laws/show/286/2015.

[2]. Архипов О.Є., Архипова Є.О. Положення про інформаційну безпеку в міжнародних стандартах // Інформаційна безпека людини, суспільства, держави.-2010.- №2(4), с.62-65.

[3]. Архипов О.Є, Архипова Є.О. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» // Информационные технологии и безопасность: основы обеспечения информационной безопасности. Материалы международной научной конференции ИТБ-2014.Сборник научных трудов. - К.: ИПРИ НАН Украины, 2014. – Выпуск 14. - 180 с., С. 18-30. ISBN: 978-966-2344-34-9.

[4]. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины, 1999.

[5]. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.

[6]. Кузьмин А. Терминология в сфере международной информационной безопасности/ А.Кузьмин, Ю.Жуков, Д.Финогенов // BIS Journal. № 3(18). – 2015. [Электронный ресурс] – Режим доступа: http://www.journal.ib-bank.ru/numbers.

[7]. ГОСТ Р ИСО/МЭК 27000-2012 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

[8]. ГОСТ Р ИСО/МЭК 27001-2006 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[9]. ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity.

[10]. Інформаційний простір України: Словник-довідник законодавчих термінів / Автор-укладач Я.О. Чепуренко. – К.: «Освіта України», 2008. – 544 с.

[11]. Войтенко Ю.А. Кибербезопасность – проблема столетия. [Электронный ресурс] – Режим доступа: http://3222.ua/ru/article/kberbezpeka-prolema_ stolttya.htm.

[12]. Каткова М. В. Понятие «информационное пространство» в современной социальной философии / М.В.Каткова //Известия Саратовского университета. 2008. Т.8. Сер. Философия.

[13]. Большая Советская Энциклопедия. Изд. 3-е. М.: «Советская Энциклопедия», 1973. Т.12, С.75. – 624 с.

[14]. Мелин А. Силы ВВС США, предназначенные для ведения боевых действий в киберпространстве, и взгляды командования на их применения / А. Мелин, С. Маринин // Зарубежное военное обозрение. - 2012. - № 6. - С. 54-59.

[15]. Мелин А. Силы кибероперацій ВМС США и основные направления их применения / А. Мелин, С. Маринин // Зарубежное военное обозрение. - 2012. - № 9. - С. 67-72.

[16]. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. [Електронний ресурс] – Режим доступу: http://s-byte.com/useful/27002.pdf.

[17]. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины, 1999.

REFERENCES

[1]. The National Security Strategy of Ukraine. President of Ukraine Decree №287 / 2015 from 25.05. 2015 [electronic resource] - Access: http://zakon5.rada.gov.ua/laws/show/286/2015.

[2]. Arkhypov A.E., Arkhipova E.A. Regulation on information security in international standards // Information security of man, society, state.-2010.-№2 (4), s.62-65.

[3]. Arkhypov O.E., Arkhipova E.A. Features an understanding of the concepts of "information security" and "safety information" // Information Technology and security: Fundamentals Provision information security. Materials International Scientific Conference ITS-2014. Collection of the Scientific Papers. - K.: IFIR National Academy of Sciences of Ukraine, 2014 - issue 14 - 180 p., S. 18-30. ISBN: 978-966-2344-34-9.
[4]. ND TIP 1.1-003-99. Terminology in the field of information protection in computer systems from unauthorized access. DSTSIP Security Service of Ukraine, 1999.
[5]. State standard R ISO / IEC 17799-2005 Information technology. Code of practice for information security management
[6]. Kuzmin A.Terminology in the sphere of international information security / A.Kuzmin, Yu.Zhukov, D.Fynogenov // BIS Journal. Number 3 (18). - 2015. [electronic resource] - Access: http://www.journal.ib-bank.ru/numbers.
[7]. State standard R ISO / IEC 27000-2012 Information technology. Security techniques. Information security management systems. Overview and vocabulary.
[8]. State standard R ISO / IEC 27001-2006 Methods and sredstva Provision security. Systems management ynformatsyonnoy security. Requirements.
[9]. ISO / IEC 27032: 2012 Information technology. Security techniques. Guidelines for cybersecurity.
[10]. The information space of Ukraine: Glossary Directory legislative terms / Author-compiler YA. O. Chepurenko. - K.: "Education of Ukraine", 2008. - 544 p.
[11]. Voytenko YU.A. Cybersecurity - the problem of the century. [Electronic resource] - Access: http://3222.ua/ru/article/kberbezpeka-problema_stolttya.htm.
[12]. Katkova M.V. The notion of "information space" in modern social philosophy / M.V.Katkova // Proceedings of Saratov University. 2008. Vol.8. Avg. Philosophy.
[13]. Great Soviet Encyclopedia. Ed. 3rd. M.: "Soviet Encyclopedia", 1973. T.12, p.75. - 624 p.
[14]. Medin A. The forces of the US Air Force, intended for combat operations in cyberspace, and looks at the command of their application / A. Medin, S.Marinin // Foreign Military Review. - 2012. - № 6. - P. 54-59.
[15]. Medin A. The forces of the US Navy cyber operations and basic directions of their application/ A. Medin, S.Marinin // Foreign Military Review. - 2012. - № 9. - P. 67-72.
[16]. Industry standard U ISMS 2.0 / ISO / IEC 27002: 2010 Information technology. Security techniques. Code of practice for information security management [Electronic resource] - Access: http://s-byte.com/useful/27002.pdf.
[17]. ND TIP 1.1-002-99. POSITION General provisions for the protection of information in computer systems from unauthorized access.. DSTSIP Security Service of Ukraine, 1999.

ПРИСТАВКА КІБЕР-: ЧИ ВСЕ ОЧЕВИДНО?

Розглянуто ситуацію, що склалася на сьогодняшний день, пов'язану зі становленням термінології в сферах інформаційної та кібербезпеки. Досліджено досить давню проблему підміни терміна «безпека інформації» терміном «інформаційна безпека». Основний акцент в статті зроблено на застосуванні термінів з приставкою кібер-. Показано, що за її допомогою виділяється клас кіберсистем, які використовуються для вирішення завдань управлінського характеру в самих різних видах діяльності. Однак у порівнянні з традиційними системами управління, в яких для вироблення управління реалізується сукупність взаємопов'язаних процесів збору, накопичення та обробки інформації, в кіберсистемах на перше місце висувається вимога безперервності й сталості управління. Ця вимога може бути виконано лише за умов забезпечення доступності, цілісності й конфідеційності вихідної інформації, яка залучається для вироблення управлінського рішення. У статті аналізуються основні властивості сучасних кіберсистем, зміст і взаємозв'язок понять «кіберпростір», «кібербезпека», «кіберзагроза».

Ключові слова: безпека інформації, інформаційна безпека, інформаційний простір, кіберсистеми, кіберпростір, кібербезпека, кіберзагроза.

PREFIX CYBER-: ALL IS OBVIOUS?

We consider the prevailing situation today, associated with the development of terminology in the field of information and cybersecurity. Abstract-old problem of substitution of the term "security of information" by the term "information security". The focus of the article is made on the use of terms with the prefix cyber-. It is shown that with the help of cyber- is distinguished class of cybersystems that are used for solving the problems of administrative character in a variety of activities. However, compared with traditional management systems that allow management implemented a set of interrelated processes of collection, storage and processing of information in the first place cybersystems extends the requirement of continuity and stability control. This requirement can be satisfied only on condition of availability, integrity and confidentiality of the source of information, attracted for the development of the administrative decision. The article analyzes the main characteristics of modern cybersystems, content and interrelation of "cyberspace" concepts "cybersecurity", "cyberthreat."

Keywords: information security, information security, information space, cybersystems, cyberspace, cybersecurity, cyberthreat.

Архипов Александр Евгеньевич, доктор технических наук, профессор кафедры информационной безопасности НТУУ «КПИ»
E-mail: sonet0515@gmail.com
Архипов Олександр Євгенійович, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ»
Arkhypov Oleksandr, Professor, Doctor of Sciences in Eng., professor of the Department of Information Defenseof National Technical University of Ukraine "Kyiv Polytechnic Institute".