НАЦІОНАЛЬНА БЕЗПЕКА

DOI: https://doi.org/10.32839/2304-5809/2019-12-76-67
УДК 004.056

Архипова Е.А.
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»

СОВРЕМЕННОЕ ПОНИМАНИЕ ТЕРМИНОВ «КИБЕРНЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ» И «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Аннотация. Целью статьи является уточнение содержания терминов кибернетическая безопасность, информационное и кибернетическое пространство. Показано, что кибернетическая безопасность является подвидом информационной безопасности и представляет собой такое состояние киберпространства, при котором обеспечивается нормальное функционирование кибернетических систем, т.е. информационных систем, предназначенных для осуществления управляющего воздействия в разных сферах человеческой деятельности. В статье приведено большое количество статистических данных, характеризующих развитие киберпространства. Показаны отличия информационной и кибернетической систем. Описана четырехуровневая модель киберпространства. Показано, что безопасность на высшем уровне основывается на инвестициях, сделанных на предыдущих уровнях. Выделены проблемы безопасности на каждом из этих уровней.

Ключевые слова: кибербезопасность, кибернетическое пространство, уровни кибернетического пространства, информационная безопасность.

Arkhypova Yevhenia
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»

MODERN UNDERSTANDING OF THE TERMS “CYBERNETIC SECURITY” AND “INFORMATION SECURITY”

Summary. There is no clear boundary between terms cybersecurity and information security, which leads to confusion, the erosion of the studied area and emergence of various difficulties among the communication parties. The purpose of the article is to clarify the content of the terms “cybersecurity”, “information space” and “cyberspace”. It is shown that cybersecurity is a subspecies of information security and represents a state of cyberspace in which the normal functioning of cyber systems is ensured, i.e. information systems intended for the implementation of control actions in various fields of human activity. It is noted that cyberspace should not be equated with the Internet, since it is a product of the functioning of not only the Internet, but also other ICTs. The article provides a large number of statistical data characterizing the main trends in the development of cyberspace in the world. It is shown that today more and more processes, including the functioning of critical infrastructure facilities, are associated with cyberspace. The expansion of the cyberspace is associated with a reduction in the cost of communications, the development of information and communication technologies, and, in particular, with an increase of the speed of information transfer. The active penetration of the Internet, including wireless communications in business processes, significantly updates the issues of cybersecurity ensuring. The differences between information and cybernetic systems are shown. It is demonstrated that any cyber system implements certain information technologies and preserves the basic features and properties of information systems. A four-level model of cyberspace is described. The physical level of cyberspace consists of the hardware and physical infrastructure necessary for the functioning of cyberspace. The logical layer consists of software and protocols embedded in the software that allow physical components to communicate. The information layer consists of information (content) that exists in cyberspace. The social level is formed by people that interact using ICTs. The levels of cyberspace are hierarchical, and security at the highest, social level is based on investments in security made at previous levels. Security issues are highlighted at each of these levels.

Keywords: cybersecurity, cyberspace, levels of cyberspace, information security.

Постановка проблемы. В последнее время все большую популярность набирает термин «кибербезопасность», который используется в одном ряду с терминами «информационная безопасность», «национальная безопасность», «безопасность информации». Глобализированное информационное пространство поднимает вопросы информационной безопасности (и кибербезопасности в частности) на новый уровень.

Анализ последних исследований и публикаций. Вопросы информационной и кибернетической безопасности исследуются такими авторами, как В. Остроухов, В. Петрик, А. Баранов, Ф. Фурашев, В. Литвиненко, И. Боднар, В. Корченко, В. Бурячок, А. Медин, С. Маринин, М. Соколов, Т. Гришина.

Отметим, что сложная военно-политическая ситуация в нашей стране существенно актуализировала вопросы информационной и кибернетической безопасности, что нашло свое отражение как в активизации научных и прикладных исследований, так и в разработке новых нормативно-правовых актов, регулирующих деятельность в этой сфере.

Выделение нерешенных ранее частей общей проблемы. Тем не менее, несмотря на достаточно большое количество публикаций, со-

держание основных терминов до сих пор остается дискуссионным, а кардинальные отличия в подходах некоторых авторов не позволяют достигнуть консенсуса. Между этими терминами не существует четкой границы, что приводит к размыванию исследуемой области и возникновению различных сложностей среди коммуницирующих сторон.

В связи с этим имеет смысл уточнить содержание терминов кибербезопасность и информационная безопасность, информационные и кибернетические системы, охарактеризовать уровни киберпространства, а также выделить проблемы безопасности на каждом из этих уровней, что и является **целью данной статьи**.

Изложение основного материала. Об информационном обществе заговорили с 60-х годов XX столетия, сейчас же отдельные исследователи заявляют о возникновении нового ноосферного образования – кибернетического общества, «управленческий механизм которого сосредоточен в основном в виртуальной сфере информационного пространства» [1]. Кибернетические системы связывают между собой различные сферы человеческой деятельности и выдвигают новые требования к ее безопасности.

Информационные системы, подвидом которых являются кибернетические системы, имеют два измерения: техническое и социальное. С одной стороны, информационные системы – это организационно-технические системы, используемые для сбора, обработки, обмена и хранения информации и включающие программные и технические средства [2]. С другой стороны, это социотехнические системы, которые формируются в результате действий пользователей информационных систем, а также процедур, которые регламентируют действия пользователей. Некоторые информационные системы являются закрытыми, не имеющими «шлюзов» для доступа в информационное пространство общего пользования. Однако даже такие системы не имеют 100% гарантии безопасности, поскольку они обслуживаются людьми, а защититься от всевозможных угроз антропогенного характера не представляется возможным. Впрочем, большая часть кибернетических (информационных) систем содержат, по крайней мере, некоторые возможности подключения к киберпространству, что существенно повышает количество угроз, которые могут на них воздействовать.

Под кибернетической системой понимается «совокупность связанных друг с другом элементов, способных воспринимать, хранить, перерабатывать информацию, а также обмениваться информацией» [3]. В общем случае кибернетическая система представляется в виде контура информационных обменов, состоящего из управляемого объекта, управляющей системы, датчиков исходной информации и каналов передачи информации. Собственно управление осуществляется путем преобразования поступившей исходной информации в сигнал управления, корректирующий состояние управляемого объекта. Таким образом, любая киберсистема реализует определенные информационные технологии и сохраняет базовые признаки и свойства информационных систем.

Определить сущность кибернетических систем можно через их функциональное предназначение: кибернетическая система – это информационная система, предназначенная для выполнения функции управления в разных сферах деятельности. В этом случае справедливо утверждение, что информационные системы – это родовое понятие по отношению к кибернетическим системам (видовое понятие). Киберсистемам как сегменту информационных систем соответствует часть информационного пространства, которая и является киберпространством [4]. Соответственно, понятие «кибербезопасность» образуется путем сужения более общего понятия – «безопасность информации». Так, стандарт ISO/IEC 27032 определяет кибербезопасность как сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

Киберсистемы функционируют в определенной, ограниченной области информационного пространства – киберпространстве; соответственно, понятие *кибербезопасность* образуется сужением более общего понятия – безопасность информации, для которого, в свою очередь, родовым понятием будет информайционная безопасность, т.е. последнее понятие является наиболее широким по объему.

Отметим, что киберпространство не следует отождествлять с интернетом, поскольку оно является продуктом функционирования не только интернета, но и других ИКТ [5]. Также следует различать киберпространство и виртуальную реальность: в отличие от первого, виртуальная реальность, как отмечает Добринская Д.Е., основана на чувственных симуляциях, а ее целью является создание иллюзии реальности. Напротив, действия в киберпространстве вполне соотносимы с объективной реальностью. Например, общение в соцсетях – это не иллюзия общения, а реальное общение с реальным человеком. Да, молодой парень спортивного телосложения может оказаться мужчиной средних лет с оплывшей фигурой, а обходительный и уступчивый продавец – коварным аферистом, но ведь и при «классическом» общении случается, что собеседники несколько приукрашивают действительность или же откровенно врут.

Расширение кибернетического пространства связано с удешевлением средств связи, развитием информационно-комуникационных технологий и, в частности, с увеличением скорости передачи информации. По материалам исследований агентства We Are Social и сервиса Hootsuite, количество пользователей интернета в 2019 году достигло 4,39 млрд человек, а темпы прироста пользователей за год увеличились с 7 до 9%, то есть за один день количество интернет-пользователей увеличивалось на 1 миллион [6]. А если верить счетчику подключений Cisco – онлайн-сервису, отслеживающему количество новых подключений к интернету – в настоящее время к сети каждую секунду подключается около 250 устройств [7].

По прогнозам компании Cisco [8], к 2022 году около 4,6 миллиардов людей и 28,5 миллиардов сетевых устройств будут подключены к интернету, а доля M2M (от англ. Machine-to-Machine, межмашинное взаимодействие) будет составлять более половины всех подключенных к интернету устройств (в 2017 – 34%).

Среднеее количество подключенных устройств на душу населения в Восточной Европе вырастет с 5,4 в 2017 до 9,4 в 2022, что является вторым по величине показателем (первое место занимает Северная Америка. Общее количество подключенных к сети устройств на душу населения по всему миру возрастет с 2,4 до 3,6 в 2022 году. Стоит отметить, что совокупный среднегодовой темп прироста количества устройств и соединений является большим (10%), чем совокупный среднегодовой темп прироста населения и интернет-пользователей вместе взятых (1 и 7% соответственно) [9].

К 2022 году будет более 12 миллиардов мобильных устройств и подключений IoT (по сравнению с девятью миллиардами в 2017 году) [10].

Около половины интернет-трафика к 2022 году будет приходиться на смартфоны, тогда как стационарные компьютеры, напротив, будут создавать 19% от его общего количества. Интересно, что в 2017 году цифры были почти зеркальные – 23% трафика приходилось на смартфоны, а 49% – на компьютеры.

Отметим, что тенденция вытеснения интернет-трафика, генерируемого стационарными компьютерами, трафиком мобильных устройств, в первую очередь смартфонов, прослеживается абсолютно во всех регионах. Во всем мире в интернет чаще выходят со смартфонов, которые генерируют больше веб-трафика, чем все прочие устройства вместе взятые [6; 10].

С киберпространством также связаны миллионы других устройств: видеокамеры, промышленные системы управления, спутники, автомобили, медицинские датчики и приборы, светофоры, фитнес-браслеты, холодильники, пылесосы, прочая бытовая техника и т.д.

По прогнозам аналитиков компании Cisco, к 2022 году 72% стационарных и мобильных устройств, подключенных к интернету, будут принадлежать потребителям, тогда как остальные 28% будут приходится на долю бизнеса. Сохраняется тенденция более быстрого роста бизнес-сегмента: на его долю приходится 12% совокупного среднегодового темпа прироста против почти 9% доли прироста потребительского сегмента [9].

Активное проникновение интернета, в том числе беспроводной связи в бизнес-процессы существенно актуализирует вопросы обеспечения кибербезопасности организаций. Быстрое расширение киберпространства, особенно за счет подключения устройств, обрабатывающих персональную и/или конфиденциальную информацию, сформировало новые вопросы в сфере обеспечения безопасности и повысило потребность в защите киберпространства. Большая часть предприятий и организаций в настоящее время зависят от информационных и кибернетических систем, которые используются для осуществления различных управленческих процессов (мониторинг, контроль, анализ, учет и т.д.). Таким образом, обеспечение надлежащего функционирования этих систем имеет решающее значение для организаций в различных секторах экономики, а обеспечение бесперебойной работы этих систем на объектах критически важной инфраструктуры является вопросом национальной, а в некоторых случаях – международной безопасности.

Таким образом, все больше процессов, в том числе функционирование объектов критической инфраструктуры, связаны с киберпространством. Д. Климент (Dave Clemente), характеризуя роль киберпространства для обеспечения функционирования объектов критической инфраструктуры, сравнивает его с «тонким слоем или нервной системой», позволяющим взаимодействовать с другими критическими секторами [11, с. 6]. По мнению ученого, такая взаимосвязанность позволяет более оперативно выделять необходимые для ликвидации проблем ресурсы, привлекая их из других секторов и даже других стран. В то же время, как это ни парадоксально, эта же информационно-техническая сопряженность усиливает риск реализации успешных атак на критическую инфраструктуру. Взломав защиту одного объекта, злоумышленник может получить доступ к другому через общую сеть. И даже исключив подобное вмешательство внешних сил, в такой ситуации увеличивается риск коррелированных сбоев, вызванных перегрузкой, так как сбой в одной части сети увеличивает нагрузку на другие.

Ряд ученых, в частности A. Klimburg, Ph. Mirtl, D. Clark, N. Choucri [12–14] рассматривают киберпространство как четырехуровневую структуру. Они выделяют такие уровни киберпространства: физический, логический, информационный и социальный. Физический уровень состоит из аппаратных устройств: кабелей, маршрутизаторов, коммутаторов, переключателей, спутников, датчиков, а также других проводных и беспроводных устройств. Логический уровень формируется программным обеспечением, включая протоколы, которые позволяют физическим компонентам работать и взаимодействовать. Информационный уровень, или уровень контента состоит из информации, которая собирается, обрабатывается, передается и сохраняется в киберпространстве. Социальный слой формируется людьми и организациями, которые взаимодействуют между собой.

Рассмотрим эти уровни детальнее. А. Климбург [13] отмечает, что физический уровень киберпространства состоит из аппаратной и физической инфраструктуры, необходимой для поддержки киберпространства. Физическая инфраструктура географически расположена в «реальном пространстве». Ядром киберпространства является интернет.

Логический уровень состоит из программного обеспечения и протоколов, встроенных в программное обеспечение [12]. На логическом уровне устройства взаимодействуют друг с другом, используя свои собственные языки и протоколы. Так, интернет – это глобальная сеть устройств, обменивающихся данными по общему протоколу передачи / интернет-протоколу (TCP / IP), представляющим собою язык, который понимает любой компьютеры. Уровни TCP и IP являются частью большого стека протоколов, который начинается с физического уровня и в конечном итоге поддерживает веб-приложения и другое программное обеспечение, взаимодействующее с людьми [15, с. 15].

Информационный слой киберпространства состоит из различных типов информации, содержащейся в информационных системах: сообщения в соцсетях, электронные письма, команды,

передаваемые через систему удаленного контроля, различные базы данных и т. д. Именно содержание информации, обрабатывающейся в системе, определяет уровень критичности объекта.

Социальный слой состоит из всех людей, использующих и формирующих киберпространство. Социальный слой – это сетевое общество, состоящее из миллионов частных, общественных, академических, правительственных, военных и деловых сетей, а также людей, которые используют эти сети [13; 15].

Киберугрозы могут повлиять на любой уровень киберпространства. Функционирование верхних уровней киберпространства зависит от работы нижних, но не наоборот. Порядок «надстройки» уровней следующий: базовым является физический уровень, далее следует логический уровень, затем – информационный и социальный уровни.

Работоспособность киберпространства на физическом уровне влияет на все остальные его уровни, в частности, если нарушено физическое соединение, то все остальные уровни также не будут функционировать. Так, в 2011 году в Армении 75-летняя пенсионерка умудрилась перерезать лопатой подземный оптоволоконный кабель, что временно сделало невозможным предоставление 90% всех интернет-услуг в стране [13].

Точно так же уязвимость на логическом уровне подрывает безопасность последующих уровней. Так, в апреле 2014 года, в середине срока, отведенного на заполнение налоговых деклараций, Канадское налоговое агентство (Canada Revenue Agency) было вынуждено остановить работу соответствующего онлайн-сервиса. Прерывание обслуживания онлайн-сервиса подачи налоговых деклараций произошло вследствие обнаружения ошибки в используемой им технологии веб-шифрования, которая позволяла получить несанкционированный доступ к любым данным на сервере или на клиентском ПК, в том числе к идентификационным куки и закрытым ключам шифрования сервера [16].

Финские специалисты по безопасности информации, обнаружившие эту ошибку, названную **Heartbleed**, и создавшие одноименный сайт для информирования общественности (http://heartbleed.com/), заявляли о существовании большой вероятности того, что она прямо или косвенно затронет многих интернет-пользователей. Как указывается на их сайте, эта ошибка в программном обеспечении, используемом для шифрования трафика в Интернете, появилась в конце 2011 года. Уязвимую библиотеку OpenSSL могли использовать различные социальные сети, коммерческие и правительственные сайты, онлайн-сервисы, сайты, через которые проводилась загрузка программного обеспечения. По оценкам специалистов в сфере ИТ-безопасности, данная уязвимость в криптографической библиотеке OpenSSL затронула около 17% веб-серверов SSL, которые используют сертификаты, выданные доверенными центрами [17].

Атаки могут также использовать человеческие слабости на социальном уровне. В марте 2011 года в результате атаки социальной инженерии были скомпрометированы токены двухфакторной аутентификации RSA, используемые компаниями по всему миру для обеспечения удаленного доступа к своим сетям. Гигант безопасности был взломан после того, как злоумышленники отправили целевые фишинговые электронные письма четырем сотрудникам его материнской компании EMC. Письма были тщательно обработаны, чтобы получатели могли их открыть и загрузить вредоносное вложение, которое было указано в строке темы как «2011 Recruitment plan.xls» [15; 17].

Нарушение безопасности на физическом уровне предполагает разрушение аппаратного обеспечения и других элементов физической инфраструктуры. Чтобы предотвратить такие атаки, владельцы инфраструктуры и сетей используют физические меры обеспечения безопасности: устанавливают решетки, заборы, электрические ограждения, различные датчики и аварийную сигнализацию, предупреждающую несанкционированное вторжение на охраняемую территорию.

На логическом уровне безопасность зависит от качества используемого программного обеспечения. Если в программном обеспечении есть ошибки, допущенные в ходе проектирования или реализации, они могут быть использованы злоумышленниками для получения доступа к информационным системам даже удаленно [15, с. 18]. Чем раньше обнаруживаются уязвимости, тем дешевле и проще их исправить и сделать программное обеспечение более защищенным.

Безопасность информационного уровня тесно связана с безопасностью логического уровня. В частности, если в используемом программном обеспечении есть уязвимости, то злоумышленники могут использовать эти уязвимости, чтобы получить доступ к информации, содержащейся в информационной системе. Для повышения уровня информационной безопасности непосредственно на информационном уровне кибернетического пространства особое внимание следует уделить информационной грамотности персонала организации, поскольку инсайдерские угрозы по-прежнему составляют существенную долю всех угроз информационной безопасности в организации. Также в организации необходимо регулярно проводить аудит информационной безопасности, оценивать информационные риски и внедрять процессы, направленные на улучшение информационной безопасности. Тем не менее, пока существуют уязвимости на предыдущих, более низких уровнях, эти способы защиты можно обойти.

В конечном итоге все кибератаки стремятся влиять на социальный слой [12]. Киберпреступники, похищающие данные банковских карт, хотят использовать эту информацию для присвоения себе чужих денежных средств. Нарушение может быть инициировано на любом уровне: злоумышленники могут использовать методы социальной инженерии, чтобы получить доступ к закрытой информации в системе от самих пользователей, либо же использовать уязвимости программного обеспечения.

Выводы. В ряде понятий *информационная безопасность, кибернетическая безопасность* и *безопасность информации*, первое понятие является наиболее общим. Кибернетическая безопасность представляет собой такое состояние киберпространства, при котором обеспечивается нормальное функционирование кибернетических

систем, т.е. информационных систем, предназначенных для осуществления управляющего воздействия в разных сферах человеческой деятельности.

В четырехуровневой модели кибернетического пространства выделяют такие уровни: физический, который состоит из аппаратных устройств: кабелей, маршрутизаторов, коммутаторов, переключателей, спутников, датчиков, а также других проводных и беспроводных устройств; логический, состоящий из программного обеспечения, которое позволяет физическим компонентам взаимодействовать; информационный, состоящий из информации (контента), которая собирается, обрабатывается, передается и сохраняется в киберпространстве; социальный уровень формируется людьми и организациями, которые взаимодействуют между собой, используя современные ИКТ. Уровни киберпространства являются иерархическими: нижние уровни первичны, обязательные для формирования последующих.

Для обеспечения безопасности киберпространства важно обеспечить безопасность на всех его уровнях, в частности принять меры для обеспечения физической целостности инфраструктуры, использовать программное обеспечение хорошего качества, внедрять различные процессы, способствующие улучшению информационной безопасности, обучать персонал правилам безопасного поведения и регулярно контролировать соблюдение этих правил. Следует отдельно отметить и тот факт, что иерархичность киберпространства проявляется и при рассмотрении вопросов безопасности: проблемы на низших уровнях обязательно будут отражаться на функционировании высших уровней, поэтому можно утверждать, что безопасность на высшем, социальном уровне основывается на инвестициях в безопасность, сделанных на более низких уровнях: физическом, логическом и информационном.

Список источников:

1. Тонконогов А.В. Кибернетическое общество как реальность XXI века. *Закон и право*. 2018. № 9. С. 23–26.
2. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: Постанова КМУ від 16.11.2002. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF (дата звернення: 26.12.2019).
3. Архипов А.Е., Архипова Е.А. Употребление определений «кибернетический» и «информационный» в сфере безопасности. *Міждисциплінарні дослідження актуальних проблем застосування інформаційних технологій в сучасному світі : матеріали V Всеукраїнської науково-практичної конференції: «Глушковські читання»* (м. Київ, 24 листопада 2016 р.). Київ, 2016. С. 28–29.
4. Архипов А.Е. Приставка кибер-: все ли очевидно? *Защита информации*. 2016. Т. 18. № 3. С. 203–209. DOI: 10.18372/2410-7840.18.10849
5. Добринская Д.Е. Киберпространство: территория современной жизни. *Вестн. Моск. ун-та. Сер. 18. Социология и политология*. 2018. Т. 24. № 1. С. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70
6. Сергеева Ю. Вся статистика интернета на 2019 год – в мире и в России. 11.02.2019. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (дата звернення: 28.11.2019).
7. The Internet of Everything. Connections Counter. Cisco. Jul 22, 2013. URL: https://www.slideshare.net/Cisco/ccs-re-ioe-connection-counter1306-v003/3-2013_Cisco_andor_its_affiliates (дата звернення: 22.11.2019).
8. VNI Forecast Highlights Tool. URL: https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html (дата звернення: 15.12.2019).
9. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. February 27, 2019. URL: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html (дата звернення: 15.12.2019).
10. 2019 Mobile VNI Forecast Update Media Release February 19, 2019. URL: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1967403 (дата звернення: 15.12.2019).
11. Clemente, D. (2013). Cyber Security and Global Interdependence: What is Critical? Chatham House. The Royal Institute of International Affairs. Online: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf (дата звернення: 12.11.2019).
12. Clark, David (2010). Characterizing cyberspace: past, present and future. *MIT/CSAIL Working Paper*, 12 March 2010. URL: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (дата звернення: 06.12.2019).
13. Klimburg, A., & Mirtl, P. (2012). Cyberspace and governance – a primer. *Working Paper*, Vol. 65. Austrian institute for international affairs. URL: https://www.ssoar.info/ssoar/handle/document/43560 (дата звернення: 09.12.2019).
14. Choucri, N., & Clark, D. (2012). Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. In *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2178586
15. Juuso Anna-Maija. Cybersecurity investment and information sharing. An Analysis of the Economic Incentives of Private Critical Infrastructure Providers: Master's Thesis. University of Oulu, 2015. 103 p.
16. Reuters (2015). E-filing of Canadian taxes shut down because of Heartbleed bug. Reuters. URL: https://www.reuters.com/article/us-tax-bug/e-filing-of-canadian-taxes-shut-down-because-of-heartbleed-bug-idUSBREA3817T20140409 (дата звернення: 15.05.2015).
17. Mutton Paul. Half a million widely trusted websites vulnerable to Heartbleed bug. 2014. URL: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

References:

1. Tonkonogov, A.V. (2018). Kiberneticheskoe obshhestvo kak real'nost' XXI veka [Cybernetic society as a reality of the 21st century]. *Law and right,* no. 9, pp. 23–26.
2. Cabinet of Ministers of Ukraine (2002). On approval of the Procedure of interaction of executive bodies on protection of state information resources in information and telecommunication systems: Resolution of the Cabinet of Ministers of Ukraine.
3. Arkhypov, A.Y., & Arkhypova, Y.A. (2016). Upotreblenie opredelenij «kiberneticheskij» i «informacionnyj» v sfere bezopasnosti [Use of the definitions of "cybernetic" and "informational" in the field of security]. *Mizhdystsyplinarni doslidzhennia aktualnykh problem zastosuvannia informatsiinykh tekhnolohii v suchasnomu*

sviti [Interdisciplinary research of current problems of application of information technologies in the modern world] (Kyiv, 24 November, 24). Kyiv, pp. 28–29.
4. Arkhypov, A.Y. (2016). Prefix cyber-: all is obvious? *Ukrainian Information Security Research Journal*, vol. 18, no. 3, pp. 203–209. DOI: 10.18372/2410-7840.18.10849 (in Ukrainian)
5. Dobrinskaya, D.E. (2018). Cyberspace: Territory of contemporary life. *Moscow State University Bulletin. Series 18. Sociology and Political Science*, vol. 24, no. 1, pp. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70 (in Russian)
6. Sergeeva, Ju. (2019). Vsja statistika interneta na 2019 god – v mire i v Rossii [All Internet statistics for 2019 – in the world and in Russia]. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (accessed: 28.11.2019).
7. The Internet of Everything. Connections Counter (2013). Cisco. URL: https://www.slideshare.net/Cisco/ccs-re-ioe-connection-counter1306-v003/3-2013_Cisco_andor_its_affiliates (accessed: 22.11.2019).
8. VNI Forecast Highlights Tool (No date). URL: https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html (accessed: 15.12.2019).
9. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. (2019) URL: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html (accessed: 15.12.2019).
10. 2019 Mobile VNI Forecast Update Media Release (2019). URL: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1967403 (accessed: 12.11.2019).
11. Clemente, D. (2013). Cyber Security and Global Interdependence: What is Critical? Chatham House. The Royal Institute of International Affairs. Online: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf (accessed: 06.12.2019).
12. Clark, David (2010). Characterizing cyberspace: past, present and future. *MIT/CSAIL Working Paper*, 12 March 2010. URL: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (accessed: 6.12.2019).
13. Klimburg, A., & Mirtl, P. (2012). Cyberspace and governance – a primer. *Working Paper*, vol. 65. Austrian institute for international affairs. URL: https://www.ssoar.info/ssoar/handle/document/43560 (accessed: 09.12.2019).
14. Choucri, N., & Clark, D. (2012). Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. In *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2178586
15. Juuso Anna-Maija (2015). Cybersecurity investment and information sharing. An Analysis of the Economic Incentives of Private Critical Infrastructure Providers: Master's Thesis. University of Oulu, 103 p.
16. Reuters (2015). E-filing of Canadian taxes shut down because of Heartbleed bug. Reuters. URL: https://www.reuters.com/article/us-tax-bug/e-filing-of-canadian-taxes-shut-down-because-of-heartbleed-bug-idUSBREA3817T20140409 (accessed: 15.05.2015).
17. Mutton Paul (2014). Half a million widely trusted websites vulnerable to Heartbleed bug. URL: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html