УДК: 004.7 DOI: 10.53816/23061456_2022_5–6_36

ПРОБЛЕМА УПРАВЛЕНИЯ ПАРАМЕТРАМИ КИБЕРПРОСТРАНСТВА В ИНТЕРЕСАХ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

THE PROBLEM OF THE CYBERSPACE PARAMETERS CONTROL FOR THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Канд. техн. наук А.А. Бречко[1], канд. техн. наук А.М. Сазыкин[2]

Ph.D. A.A. Brechko, Ph.D. A.M. Sazykin

[1]Академия ФСО России (г. Орёл), [2]АО «НПО Спецматериалов»

В статье произведен анализ условий функционирования субъектов критической информационной инфраструктуры, сформулирована новая научная проблема, решение которой вносит значительный вклад в развитие безопасности страны. Субъекты критической информационной инфраструктуры осуществляют выполнение критически важных процессов, нарушение которых создает угрозу безопасности Российской Федерации. Многие процессы в той или иной степени интегрированы в киберпространство, и степень их интеграции растет. Множественные разнородные субъекты управления осуществляют свою деятельность на основе статистических показателей киберпространства, при этом цели отдельных пользователей, в том числе субъектов критической информационной инфраструктуры, при выработке управленческих решений не учитываются. В этой связи актуализируется проблема управления параметрами киберпространства в интересах субъектов критической информационной инфраструктуры Российской Федерации.

Ключевые слова: критическая информационная инфраструктура, киберпространство, система управления.

The article analyzes the conditions of functioning of the subjects of the critical information infrastructure, a new scientific problem is formulated, the solution of which makes a significant contribution to the development of the country's security. The subjects of the critical information infrastructure carry out the implementation of critical processes, the violation of which poses a threat to the security of the Russian Federation. Many processes are more or less integrated into cyberspace and the degree of their integration is growing. Multiple heterogeneous management entities carry out their activities on the basis of statistical indicators of cyberspace, while the goals of individual users, including subjects of critical information infrastructure, are not taken into account when making management decisions. In this regard, the problem of managing the parameters of cyberspace in the interests of the subjects of the critical information infrastructure of the Russian Federation is being updated.

Keywords: critical information infrastructure, cyberspace, management system.

Субъектами критической информационной инфраструктуры (КИИ) Российской Федерации являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, в банковской и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности; российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [1].

Субъекты КИИ весьма разнородны, обладают сложной структурой, элементы которой, как правило, широко территориально распределены, и, главное, обеспечивают выполнение критически важных процессов (управленческих, технологических, производственных, финансово-экономических и др.). Нарушение таких процессов может повлечь в числе прочих [2]:

– причинение ущерба жизни и здоровью людей;

– нарушение условий международных договоров Российской Федерации;

– возникновение значительного ущерба бюджетам Российской Федерации;

– прекращение или нарушение проведения банковских операций;

– вредные воздействия на окружающую среду;

– снижение показателей государственного оборонного заказа;

– прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, объектов транспортной инфраструктуры, сетей связи, государственных органов, государственных или ведомственных пунктов управления, информационной системы в области обеспечения обороны страны.

Например, система водоснабжения Санкт-Петербурга представляет собой комплекс взаимосвязанных инженерных сооружений, обеспечивающих бесперебойную подачу потребителям питьевой воды. В состав комплекса входят 9 водопроводных станций, 187 повысительных насосных станций, сеть трубопроводов протяженностью 7414 км, 2 завода по производству гипохлорита натрия [3]. Нарушение процесса обеспечения города чистой (безопасной) водой может стать причиной катастрофических последствий.

В связи с тем, что процессы, обеспечиваемые субъектами КИИ, являются сложными, деятельность субъектов характеризуется частой сменой местоположения и роли их элементов, генерацией разнородного трафика с переменной интенсивностью, высокой чувствительностью к нарушениям конфиденциальности, доступности и целостности обрабатываемой информации.

Традиционные иерархические системы управления характеризуются безоговорочным владением объектом управления, единоличной реализацией всех функций, расчетом на предельную прогнозируемую нагрузку, соответствием системы управления целям вышестоящей системы. Традиционные системы управления разрабатывались на единой и контролируемой технологической платформе.

В противоположность традиционным системам управления, субъекты КИИ, которые являются организационно-техническими системами управления, не эксплуатируют какую-то отдельную изолированную техническую систему, будь то информационная система, информационно-телекоммуникационная сеть или автоматизированная система управления. Напротив, прослеживается объединение таких систем друг с другом и, в конечном счете, их интеграция в киберпространство. Именно конвергенция технических систем, переход процессов в общее технологическое пространство является ключом и важнейшим аспектом исследуемой проблематики.

Киберпространство

Киберпространство — искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления, при этом свойства киберпространства зависят как от характеристик собственных

элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [4].

Ядром киберпространства является глобальная сеть Интернет, которая развивается в соответствии с основными принципами, заложенными в RFC 1958:

– принцип функциональной совместимости;

– принцип открытости;

– принцип сквозной связи;

– принцип отсутствия централизованного управления.

Помимо формальных принципов развития киберпространства существует ряд объективных (естественных) принципов, в основу которых положено получение финансовой прибыли.

Учитывая это, в отношении киберпространства сформулированы следующие утверждения:

– киберпространство разделено между множеством собственников, ключевые из которых международные;

– киберпространство функционирует не менее чем в 200 юрисдикциях;

– качество предоставляемых услуг основывается на статистическом подходе, без учета интересов конкретного пользователя;

– решения по управлению киберпространством основываются на средних эксплуатационных показателях;

– маршрутизация должна обеспечить загрузку эксплуатируемого оборудования, а не выполнение требований отдельного пользователя.

Структурной единицей киберпространства является автономная система — сеть под единым административным управлением. Всего в мире зарегистрировано 96878 автономных систем, из которых 6281 расположены в России. За каждой автономной системой закреплено множество уникальных IP-адресов.

Общая емкость IPv4 адресного пространства составляет около 4 млрд адресов, которая практически исчерпана. Наибольшее количество распределено между США (1,6 млрд, 43,7 %), Китаем (340 млн, 9,25 %), и Японией (190 млн, 5,16 %). На долю России приходится 46 млн IPv4 адресов, что составляет 1,25 % от их общего количества.

Емкость IPv6 адресного пространства практически неисчерпаема и в настоящее время используется в меньшей степени. Потенциально существует более 2128 IPv6 адресов.

В табл. 1 представлены крупнейшие автономные системы под управлением российских юридических лиц.

Крупнейшая автономная система — сеть ПАО «Ростелеком» — состоит из магистральных линий, протяженностью около 500 тыс. км, построенных на волоконно-оптических линиях с использованием SDH- и DWDM технологий, а также местных сетей, общей протяженностью свыше 2,6 млн км. Магистральные линии соединяются через транзитные междугородные и международные узлы связи с сетями связи иностранных государств. Сеть имеет прямые стыки со 190 сетями в 70 странах.

Помимо прямого соединения сетей через пограничные маршрутизаторы зачастую операторы связи используют точки обмена трафиком — сетевую инфраструктуру, предназначенную для оперативной организации соединений и межоператорского обмена трафиком (пиринга). Как правило, точка обмена трафиком состоит из нескольких территориально разнесенных узлов связи, соединенных высокоскоростными магистральными линиями связи.

Крупнейшими точками обмена трафиком на территории России являются MSK-IX, DATAIX, CLOUD-IX, W-IX, RED-IX, SIBIR-IX, SEA-IX, PITER-IX и CRIMEA-IX. Наиболее крупная —

Таблица 1

Крупнейшие автономные системы под управлением Российских юридических лиц

№	Автономная система	Владелец	Количество IPv4 адресов	Процент от общего количества
1	AS 12389	ПАО «Ростелеком»	9 214 336	0,231 %
2	AS 8402	ПАО «Вымпелком»	2 304 512	0,058 %
3	AS 12714	ООО «Нэт бай Нет Холдинг»	1 232 896	0,031 %
4	AS 3216	ПАО «Вымпелком»	1 210 368	0,031 %
5	AS 8359	ПАО «Мобильные телесистемы»	1 160 448	0,03 %

MSK-IX, представляет собой соединенные между собой узлы производительностью 8 Тбит/с каждый, находящиеся в Москве, Санкт-Петербурге, Ростове-на-Дону, Ставрополе, Самаре, Казани, Екатеринбурге, Новосибирске, Владивостоке и Риге.

Система управления киберпространством

Глобальная архитектура управления киберпространством в своем функциональном, структурном и институциональном аспектах сложилась в 1990–2000 гг. [5]. Далее представлен перечень основных субъектов управления.

IEEE (Institute of Electrical and Electronics Engineers — Институт инженеров электротехники и электроники) [6]. Некоммерческая ассоциация, расположенная в США. Разрабатывает стандарты по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей.

ITU (International Telecommunication Union — Международный союз электросвязи) [7]. Международная организация, определяющая рекомендации в области телекоммуникаций и радио. Главный офис находится в Швейцарии.

ISOC (Internet Society — Сообщество Интернета) [8]. Некоммерческая корпорация, расположенная в США. Поддерживает и способствует развитию Интернета, для чего создает и поддерживает дочерние сообщества (в том числе Российское отделение [9]), продвигает технологии и стандарты. Деятельность сообщества финансируется в основном из взносов юридических и физических лиц. Обладает правами на все документы RFC.

IAB (Internet Architecture Board — Совет по архитектуре Интернета) [10]. Организация, не имеющая юридического лица (техническая координационная площадка), находится под управлением ISOC и выступает от его имени по курируемым вопросам. Обеспечивает техническое развитие Интернета, связанное с его архитектурой, включая разработку протоколов и стандартов.

IETF (Internet Engineering Task Force — Рабочая группа по проектированию Интернета) [11]. Также не имеет юридического лица и находится под управлением ISOC. Непосредственно участвует и возглавляет собрание рабочих групп по разработке спецификаций, стандартов и соглашений; выносит принятые решения на рассмотрение IESG (The Internet Engineering Steering Group — Группа по выработке инженерного регламента Интернета), которая также находится под управлением ISOC.

ICANN (Internet Corporation for Assigned Names and Numbers — Корпорация Интернета по присвоению имен и номеров) [12]. Некоммерческая корпорация, расположенная в США. Осуществляет управление глобальным распределением доменных имен (DNS) и IP-адресов.

IANA (Internet Assigned Numbers Authority — Администрация адресного пространства Интернет) [13]. Департамент в структуре ICANN. Осуществляет администрирование корневых серверов DNS, распределяет диапазоны IP-адресов региональным интернет-регистраторам.

RIR (Regional Internet Registry — Региональный интернет регистратор). Ряд организаций (ARIN, RIPE NCC, APNIC, LACNIC, AfrNIC), занимающихся вопросами адресации и маршрутизации в сети Интернет. Региональным интернет-регистратором, осуществляющим свою деятельность, в том числе на территории России, является RIPE NCC.

RIPE NCC (Réseaux IP Européens Network Coordination Centre — Сетевой координационный центр Европейских IP сетей) [14]. Некоммерческая организация, расположенная в Нидерландах. Поддерживает работу Интернета в Европе, Центральной Азии и на Ближнем Востоке. Предоставляет IP-адреса и номера автономных систем местным интернет-провайдерам и крупным организациям.

Крупнейшими организациями (операторами связи), владеющими телекоммуникационными ресурсами на территории России являются [15]: ПАО «Ростелеком», ПАО «Вымпелком», ООО «Нэт Бай Нэт Холдинг», ПАО «МТС», ПАО «Мегафон», АО «Компания ТрансТелеКом». В пределах своей инфраструктуры операторы связи имеют законные полномочия распоряжаться телекоммуникационными ресурсами по своему усмотрению (в рамках ограничений, установленных регуляторами).

Основу сетевой инфраструктуры операторов связи составляет сетевое оборудование коммутации и маршрутизации. Крупнейшими производителями такого оборудования являются компании: Cisco Systems (США), Hewlett-Packard (США), Alcatel-Lucent (Франция), Juniper Networks (США), Huawei (Китай). Как правило, производители не

предоставляют полномочий для полного управления своим оборудованием, а предустановленное программное обеспечение является закрытым.

На территории России основные структуры, управляющие киберпространством представлены следующим перечнем: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) занимается выработкой и реализацией государственной политики и нормативно-правовым регулированием; Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России) реализует государственную политику, организует межведомственную координацию и взаимодействие, осуществляет специальные и контрольные функции в области государственной безопасности, в том числе в области кибербезопасности; Федеральная служа безопасности Российской Федерации (ФСБ России) отвечает за обеспечение безопасности страны, в том числе в телекоммуникационной сфере.

Нелегитимное управление киберпространством осуществляют антагонистические системы управления, в числе которых не только различные хакерские группировки, известнейшие из которых «Anonymous», «Шалтай-Болтай», «Legion of Doom», «LulzSec», но и силы кибероперациий иностранных государств. Такое управление представляет собой изменение параметров атакуемых элементов киберпространства.

Также субъектами управления киберпространством, деятельность которых носит стохастический характер, можно считать множество его пользователей, а также природные (техногенные) явления. Одни оказывают воздействие на состояние киберпространства путем генерации трафика, другие нарушают физическую целостность инфраструктуры.

Таким образом, управление киберпространством осуществляется разнородными субъектами и может отличаться уровнем, целью, масштабом и скоростью воздействия, типом управляемых параметров, периодичностью управления, а также силой и длительностью эффекта.

В табл. 2 и 3 представлены характеристики процесса управления киберпространством различными субъектами.

Проблема исследования

В масштабах киберпространства отдельный субъект КИИ представляет собой абонен-

Таблица 2

Характеристики процесса управления киберпространством (часть 1)

Глобальные институты управления (IEEE, ITU, ISOC, IAB, IETF)	Функциональные институты управления (ICANN, IANA, RIR)	Операторы связи (владельцы автономных систем)	Крупнейшие производители оборудования
Уровень управления			
Глобальный	Стратегический	Оперативный	Глобальный, стратегический
Цель управления			
Поддержание работоспособности интернета	Поддержание работоспособности интернета	Обеспечение услугами потребителей	Техническое обеспечение операторов связи
Тип управляемых параметров			
Концептуальные	Технические	Технические	Технические
Периодичность управления			
Редко	Редко	Часто	Редко
Сила воздействия			
Маленькая	Маленькая	Большая	Большая
Длительность эффекта			
Очень высокая	Высокая	Низкая	Высокая
Масштаб воздействия			
КП	КП, регион	АС	КП, регион, АС
Скорость воздействия			
Низкая	Средняя	Высокая	Низкая

Таблица 3

Характеристики процесса управления киберпространством (часть 2)

Российские регуляторы	Антагонистические системы управления	Множество пользователей (абонентов)	Природные воздействия
Уровень управления			
Стратегический, оперативный	Тактический	Тактический	Тактический
Цель управления			
Обеспечение функционирования российского сегмента КП	Нарушение функционирования субъектов КИИ, хищение, модификация информации	Стохастическая	Стохастическая
Тип управляемых параметров			
Концептуальные	Технические	Технические	Физические
Периодичность управления			
Редко	Постоянно	Постоянно	Редко
Сила воздействия			
Средняя	Большая	Средняя	Сильная
Длительность эффекта			
Высокая	Низкая	Средняя	Низкая
Масштаб воздействия			
Регион	АС, узел, линия	КП, регион, АС	Фрагмент АС, узел, линия
Скорость воздействия			
Низкая	Очень высокая	Высокая	Высокая

та, который не оказывает значительного влияния на его состояние. Цели субъекта КИИ не коррелируют с целями субъектов управления киберпространством и, главное, не учитываются ими при выработке и реализации управленческих решений.

Отсутствие учета целей субъектов КИИ при управлении параметрами киберпространства, особенно принимая во внимание деятельность антагонистических систем управления, может привести киберпространство в такое состояние, при котором нарушается требуемое течение критических процессов, что создает прямую угрозу безопасности Российской Федерации.

Учитывая отсутствие в науке и технике теоретических и практических решений по управлению параметрами киберпространства субъектами КИИ, сформулирована новая научная проблема — проблема управления параметрами киберпространства в интересах субъектов критической информационной инфраструктуры в условиях существующей неоднородной децентрализованной многоуровневой системы управления киберпространством.

Решение указанной проблемы имеет важное значение, которое внесет значительный вклад в развитие безопасности страны. Для чего требуется разработать теоретические положения (принципы, концепции, модели, методы, методики, способы, средства) по управлению параметрами киберпространства силами субъектов КИИ.

Опираясь на архитектуру классической системы управления, разработана концептуальная схема управления киберпространством (рисуснок).

Множество систем управления различных уровней, представленных на рисунке блоком «Источники воздействий», на основе собственных целей F осуществляют воздействия $Y(t)$.

Подсистема сбора выполняет добывание информации о воздействиях систем управления $Y(t)$ и о состоянии киберпространства $X(t)$, при этом предоставляя подсистеме принятия решений полученные данные $X^*(t)$ и $Y^*(t)$.

Подсистема принятия решений на основе собственных целей S и информации о сложившейся ситуации $I(t)=\left[X^*(t), Y^*(t)\right]$ с помощью алгоритма φ вырабатывает управляющее воздействие $U(t)=\varphi\left(I(t), S\right)$.

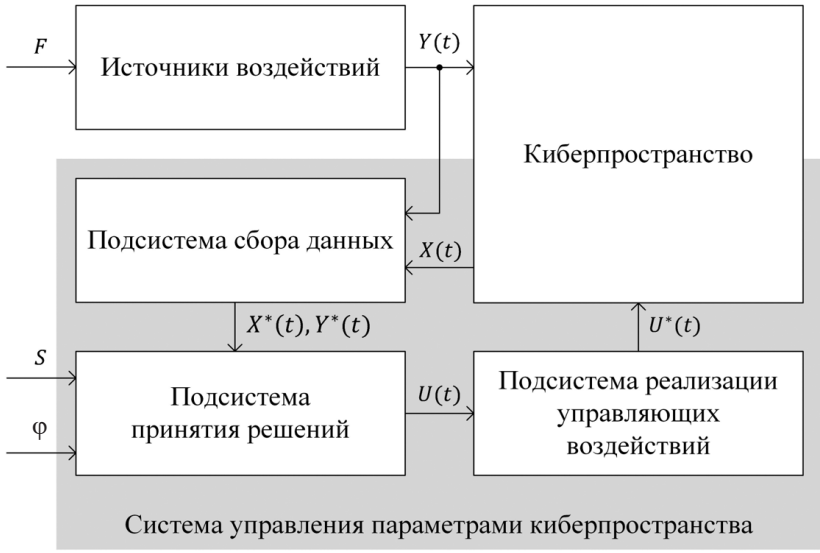

Рис. Концептуальная схема управления киберпространством

Подсистема реализации управляющих воздействий на основе сгенерированного решения управляет параметрами киберпространства, непосредственно осуществляя воздействия $U^*(t)$.

Направление дальнейших исследований

Для решения проблемы управления параметрами киберпространства в условиях существующей неоднородной децентрализованной многоуровневой системы управления киберпространством необходимо разработать комплекс взаимоувязанных теоретических положений, которые направлены на решение следующих частных задач.

1. Разработка концепции управления параметрами киберпространства.

2. Формулировка целей управления параметрами киберпространства.

3. Декомпозиция киберпространства на управляемые сегменты.

4. Моделирование киберпространства.

5. Разработка методов, методик, способов и средств сбора данных о состоянии киберпространства и реализуемых на него воздействиях.

6. Разработка методов, методик, способов и средств выработки и реализации управляющих воздействий.

Выводы

1. Киберпространство является сложнейшей технологической системой, созданной и развивающейся на основе ряда принципов, ключевым из которых — принцип децентрализованного управления.

2. Субъекты КИИ и критически важные процессы, которые они обеспечивают, по большей части интегрированы в киберпространство, и степень интеграции растет.

3. Цели субъектов КИИ не коррелируют с целями субъектов управления киберпространством и, главное, не учитываются ими при выработке и реализации управленческих решений.

4. Отсутствие учета целей субъектов КИИ при управлении параметрами киберпространства может привести его в такое состояние, при котором нарушается требуемое течение критических процессов.

5. Актуализируется проблема управления параметрами киберпространства в интересах субъектов критической информационной инфраструктуры в условиях существующей неоднородной децентрализованной многоуровневой системы управления киберпространством.

6. Решение проблемы требует разработки теоретических положений (принципы, концепции, модели, методы, методики, способы, средства) по управлению параметрами киберпространства.

Литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической ин-

формационной инфраструктуры Российской Федерации». URL: http://www.consultant.ru/ (дата обращения 08.08.2021).

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». URL: http://www.consultant.ru/ (дата обращения 08.08.2021).

3. Официальный сайт ГУП Водоканал Санкт-Петербурга. URL: http://www.vodokanal.spb.ru/ vodosnabzhenie/struktura_vodosnabzheniya (дата обращения 08.08.2021).

4. Стародубцев Ю.И. Структурно-функциональная модель киберпространства / Ю.И. Стародубцев, П.В. Закалкин, С.А. Иванов // Вопросы кибербезопасности, 2021. № 4 (44). С. 16–24.

5. Демидов О. Глобальное управление интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества. — М.: Альпина Паблишер, 2016. 198 с.

6. Официальный сайт IEEE. URL: https://www.ieee.org/ (дата обращения 08.08.2021).

7. Официальный сайт ITU. URL: https://www.itu.int/ (дата обращения 08.08.2021).

8. Официальный сайт Internet Society. URL: https: //www.internetsociety.org/ (дата обращения 08.08.2021).

9. Официальный сайт ISOC. URL: http://isocru.org/ (дата обращения 08.08.2021).

10. Официальный сайт IAB. URL: https://www.iab.org/ (дата обращения 08.08.2021).

11. Официальный сайт IETF. URL: https://www.ietf.org/ (дата обращения 08.08.2021).

12. Официальный сайт ICANN. URL: https://www.icann.org/ (дата обращения 08.08.2021).

13. Официальный сайт IANA. URL: https://www.iana.org/ (дата обращения 08.08.2021).

14. Официальный сайт RIPE NCC. URL: https: //www.ripe.net/ (дата обращения 08.08.2021).

15. Официальный сайт IDIDB. URL: https: //www.ididb.ru/autnum/ (дата обращения 08.08.2021).

References

1 Federal Law № 187-FZ of 26.07.2017 «On the security of the Critical Information Infrastructure of the Russian Federation». URL: http://www.consultant.ru/ (accessed 08.08.2021).

2. Resolution of the Government of the Russian Federation № 127 of February 8, 2018 «On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as the list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values». URL: http://www.consultant.ru/ (accessed 08.08.2021).

3. The official website of the State Unitary Enterprise Vodokanal of St. Petersburg. URL: http://www.vodokanal.spb.ru/ vodosnabzhenie/struktura_vodosnabzheniya (accessed 08.08.2021).

4. Starodubtsev Yu.I. Structural and functional model of cyberspace / Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. // Questions of cybersecurity, 2021. № 4 (44). P. 16–24.

5. Demidov O. Global Internet governance and security in the field of ICT use: Key challenges for the world community. — Moscow: Alpina Publisher, 2016. 198 p.

6. IEEE official website. URL: https://www.ieee.org/ (accessed 08.08.2021).

7. ITU official website. URL: https://www.itu.int/ (accessed 08.08.2021).

8. Internet Society official website. URL: https://www.internetsociety.org/ (accessed 08.08.2021).

9. ISOC official website. URL: http://isocru.org/ (accessed 08.08.2021).

10. IAB official website. URL: https://www.iab.org/ (accessed 08.08.2021).

11. IETF official website. URL: https://www.ietf.org/ (accessed 08.08.2021).

12. The official website of ICANN. URL: https://www.icann.org/ (accessed 08.08.2021).

13. IANA official website. URL: https://www.iana.org/ (accessed 08.08.2021).

14. RIPE NCC official website. URL: https://www.ripe.net/ (accessed 08.08.2021).

15. IDIDB official website. URL: https://www.ididb.ru/autnum/ (accessed 08.08.2021).