ЭВОЛЮЦИЯ СИСТЕМ УПРАВЛЕНИЯ КИБЕРПРОСТРАНСТВОМ

Закалкин П.В.[1]

Цель исследования: *выделение основных систем, осуществляющих управление киберпространством и ключевых элементов, управление которыми позволит контролировать заданный сегмент киберпространства.*

Метод исследования: *теория сложных систем; синергетика.*

Результат: *В работе рассмотрены основные управляющие системы, играющие ключевую роль в управлении киберпространством, выделены структурные элементы киберпространства и их взаимосвязи между собой. Рассмотрены региональные и локальные интернет регистраторы, представлен их граф связанности, а также граф связанности по странам. На основе проведенного исследования представлено авторское видение организационной структуры системы управления киберпространством (применительно к доменным именам и IP-адресам). Рассмотрены автономные системы и точки обмена трафиком, на примерах приведена структура внешней связанности автономных систем и ее изменение со временем. Представлены крупнейшие телекоммуникационные альянсы, оказывающие влияние на деятельность операторов связи (непосредственно или косвенно) и, в конечном итоге, на получаемые конечными потребителями набор ресурсов и услуг (а также их стоимость), предоставляемых телекоммуникационными операторами.*

Научная новизна: *рассмотренная структура системы управления киберпространством позволила выделить основные системы, осуществляющие управление киберпространством и ключевые элементы, управление которыми позволит контролировать заданный сегмент киберпространства.*

Ключевые слова: *киберпространство, автономная система, управление, интернет регистраторы, точка обмена трафиком, телекоммуникационные альянсы, граф связанности, ICANN.*

DOI:10.21681/2311-3456-2022-1-76-86

Введение

Движущей силой эволюции систем управления киберпространством является возможность существенного, а в ряде случаев и принципиального влияния на социальные, экономические и военно-политические процессы любого масштаба. В процессе управления киберпространством задействовано большое количество участников с разной степенью участия и влияния на параметры киберпространства.

Интеграция сетей мировых операторов связи, инфокоммуникационных систем, систем навигации, мониторинга, информационной инфраструктуры, информационных и телекоммуникационных технологий, технологий их сопряжения и управления и т.д. воедино привело к формированию пространства планетарного масштаба – киберпространства. Используя ресурсы киберпространства, осуществляется управление организационными и технологическими процессами, реализованными в рамках объектов и субъектов критической инфраструктуры государства, в том числе банковской системой, логистическими процессами, энергетикой, водоснабжением, медициной, образованием и др. [1-3]. Использование этих систем, ресурсов и услуг, предоставляемых киберпространством, сделало их мишенью как киберкомандований иностранных государств и организованных хакерских группировок, так и одиночных хакеров, регулярно осуществляющих мониторинг и деструктивные программные воздействия на инфраструктуру государств[1] [4-7].

Возможность удаленных деструктивных воздействий на критическую инфраструктуру государств позволяет без фактического ввода вооруженных сил на территорию противостоящего государства и объявления войны дестабилизировать его экономику и инфраструктуру [8-12].

Управление параметрами киберпространства возможно осуществлять как в общих интересах (в равных долях и пропорциях), так и путем изменения параметров киберпространства в интересах одной из сторон. Соответственно, сам факт возможности управления (в той или иной степени) столь сложным трансграничным пространством мирового масштаба, помимо финансовой выгоды и военного преимущества позволяет оказывать влияние на геополитические процессы, протекающие как в мире в целом, так и в отдельных странах [13-16].

1 1) Positive Research 2020 Сборник исследований по практической безопасности 2020 // Positive Technologies. С. 274. Официальный сайт Positive Technologies.

2) Топ угроз ИБ в корпоративных сетях. Результаты мониторинга сетевого трафика в 2020 году // Positive Technologies. 2021. 9 с.

3) Кибербезопасность 2020-2021. Тренды и прогнозы // Positive Technologies. 2021. 25 с.

1 Закалкин Павел Владимирович, кандидат технических наук, докторант Военной академии связи, Санкт-Петербург, Россия. E-mail: pzakalkin@mail.ru

Единого центра управления киберпространством не существует, но борьба за количество параметров, степенью управления ими, а также за перенос каналов управления на подконтрольную территорию и т.д. ведется постоянно. Уже сейчас заметен значительный перекос количества управляемых параметров и каналов управления в пользу США.

Учитывая высокую сложность, динамичность изменения состава, структуры и протекающих процессов в киберпространстве, множества разнородных, территориально распределенных элементов, являющихся его составляющими, а также распределенный характер его ресурсов, киберпространство пока не имеет единого центра управления, а сам процесс управления реализуется большим количеством участников с разной степенью участия и влияния на параметры киберпространства [17-20].

В общем случае процесс управления – это сбор информации о состоянии управляемого объекта, принятие решения о желательном состоянии и последующее изменение параметров, переводящих объект управления в желательное состояние. Соответственно, для осуществления управления киберпространством необходимо иметь доступ к управлению ключевыми параметрами и осуществлять их изменение быстрее чем множество противоборствующих сторон.

В зависимости от выполняемых задач управление можно разделить на:

Оперативное (текущее) управление – непосредственное управление, осуществляемое в текущих условиях и решающее текущие задачи. Управление пространством IP-адресов, управление службой единого времени и синхронизации, доменами верхнего уровня, параметрами протоколов и т.д.

Среднесрочное управление – направлено на решение среднесрочных задач. Например, оборудование территории в отношении связи (создание новых узлов, выбор оптимальных мест их размещения, строительство региональной кабельной инфраструктуры, перевод других элементов киберпространства региона под свою юрисдикцию), выделение пулов IP-адресов, регистрация автономных систем и т.д.

Стратегическое управление – направлено на долгосрочные цели и действия. Стратегии развития киберпространства, оснащение территории в области связи (строительство межконтинентальной кабельной инфраструктуры, создание точек обмена трафиком, хостов-реплик DNS серверов и т.д.), разработка новых протоколов, стандартов и оборудования, позволяющего их реализовать, лицензирование, технологическое опережение конкурентов и т.д.

Целью данной статьи является выделение основных систем, осуществляющих управление киберпространством и ключевых элементов, управление которыми позволит контролировать заданный сегмент киберпространства.

Далее рассмотрим существующую иерархическую структуру управления киберпространством, вершину которой представляет организация ICANN (Internet Corporation for Assigned Names and Numbers) и ее дочерняя структура IANA (Internet Assigned Numbers Authority).

ICANN, IANA и корневые DNS сервера

Основными функциями ICANN является регулирование вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования киберпространства. Помимо этого, ICANN координирует функции IANA по управлению пространствами IP-адресов, доменами верхнего уровня и параметрами протоколов, используемых в киберпространстве.

Формально ICANN является независимым сообществом заинтересованных сторон-волонтеров со всего мира, главной целью которых является обеспечение стабильности, безопасности и единства глобального интернета[2]. Однако, вопрос с независимостью ICANN является достаточно сложным и требует рассмотрения исторического аспекта появления ICANN.

До создания ICANN, управление пространством IP-адресов и доменов верхнего уровня осуществляло Правительство США в лице Министерства торговли США. В 1998 году Правительством США была создана ICANN и формально США отошли от управления. Однако, Правительство США продолжало сохранять фактический контроль над ICANN посредством возобновляемого контракта с министерством торговли США и Национальным управлением информации и связи (NTIA). Согласно этому контракту ICANN управляла адресным пространством интернета (доменными зонами и IP-адресами) через структуру IANA, подконтрольную NTIA. ICANN должна была согласовывать ключевые решения с подразделением Министерства торговли США, которое, в свою очередь, могло воспользоваться правом вето.

Естественно, такая ситуация не устраивала мировое сообщество. Например, регуляторы РФ в области телекоммуникаций опасались того, что ICANN подконтрольна американским властям и, во-первых, может по их приказу нарушить работу российского сегмента киберпространства или заблокировать домены верхнего уровня – ru и рф, а, во-вторых, помогать осуществлять США разведывательную деятельность в киберпространстве. Аналогичной позиции придерживался ряд других стран, в том числе и Китай.

Раскрытие ряда документов, в том числе по шпионству США за высшим руководством Европейских стран, показало обоснованность этих опасений и вынудили США сделать вид, что они идут на уступки. Так, в 2016 году ICANN официально обрел независимость. При передаче управления ICANN – США выставили ряд условий, основными из которых были:

- принципы работы ICANN должны быть разработаны мировым интернет-сообществом без участия правительств других государств;
- решение о соответствии разработанной системы принципов предъявляемым требованиям единолично принимает правительство США.

2 Официальный сайт Internet Corporation for Assigned Names and Numbers. URL: https://www.icann.org/ (дата обращения 10.10.2021 г.)

Таблица 1

Перечень корневых DNS серверов

Имя хоста	Управляющая организация	Страна
a.root-servers.net	VeriSign, Inc.	США
b.root-servers.net	University of Southern California (ISI)	США
c.root-servers.net	Cogent Communications	США
d.root-servers.net	University of Maryland	США
e.root-servers.net	NASA (Ames Research Center)	США
f.root-servers.net	Internet Systems Consortium, Inc.	США
g.root-servers.net	US Department of Defense (NIC)	США
h.root-servers.net	US Army (Research Lab)	США
i.root-servers.net	Netnod	Швеция
j.root-servers.net	VeriSign, Inc.	США
k.root-servers.net	RIPE NCC	Нидерланды
l.root-servers.net	ICANN	США
m.root-servers.net	WIDE Project	Япония

Согласование и выработка плана передачи управления ICANN заняло около двух лет, при всем этом, ICANN как организация зарегистрирована в США, находится под их юрисдикцией и вынуждена выполнять их законы.

Приобретение ICANN независимости еще больше усложнило ситуацию с управлением киберпространством. Получается, что киберпространством управляет некая некоммерческая организация, работающая по американскому праву, созданная Правительством США, решающая все судебные вопросы в судах США и в настоящий момент времени официально независимая от правительств всех стран.

Данная ситуация имеет множество неоспоримых плюсов для США:

- прежде всего это снятие с себя ответственности за отказ функционирования любого из сегментов киберпространства, т.к. теперь они официально им не управляют;
- все претензии по качеству работы ICANN можно предъявить только ICANN и решаться они будут по законам США;
- наличие созданной собственными руками организации, формально независимой, лояльно настроенной и функционирующей по принципам, согласованным с США. Учитывая, что ICANN формировалось и существовало под юрисдикцией США, с уверенностью можно утверждать, что множество сотрудников являются или действующими, или бывшими сотрудниками спецслужб. Данный факт позволяет и дальше успешно вести работу по разведке в киберпространстве.

Таким образом, произошло так называемое «размывание» ответственности. Фактически ключевые структуры управления киберпространством находятся в руках некой некоммерческой организации, порядок финансирования, делегирования членов в правление, ответственность и т.д. не определены, а принципы функционирования согласованы и утверждены правительством США. При этом организация имеет ключевые права в области управления киберпространством, ответственности как таковой не несет, а все претензии решаются в судах США и по их законам.

Аналогичная ситуация наблюдается и в координируемыми ICANN корневыми DNS серверами, осуществляющими адресацию в киберпространстве. В мире всего 13 корневых DNS серверов управляемых 12-ю независимыми организациями (таблица 1). Подавляющее большинство корневых DNS серверов находится на территории США и соответственно подчиняется его законодательству.

Каждый корневой DNS сервер имеет множество хостов-реплик (суммарно насчитывается 1404 хоста), расположенных в разных местах киберпространства и имеющих один и тот же IP-адрес. Порядка 260 хостов-реплик находятся на территории США, это количество является наибольшим среди всех стран. На территории РФ нет корневых серверов, а имеющиеся 14 хостов-реплик принадлежат шести корневым серверам (e.root, f.root, i.root, j.root, k.root, l.root) к оставшимся семи корневым серверам или к их репликам доступ осуществляется через зарубежные узлы.

В случае усложнения военно-политической обстановки возможность доступа к репликам корневых серверов, не расположенных на территории РФ будет целиком зависеть от зарубежных государств и с большой долей вероятности в этом доступе будет отказано

(либо будет приложен максимум усилий по усложнению этого доступа). Помимо этого, встает вопрос об идентичности содержания хостов-реплик, расположенных как на территории РФ, так и за рубежом, оригинальным корневым серверам.

Конечно, организации, управляющие корневыми серверами, позиционируют себя как независимые некоммерческие организации и, как особо подчеркивается, финансово и юридически не зависят от ICANN. Однако, среди обладателей корневых серверов есть Министерство обороны США, NASA, Сухопутные войска США, а также университеты, занимающиеся (в той или иной мере) подготовкой сотрудников киберпродразделений США. Это в явном виде указывает на то, что Правительство США до сих пор принимает участие в управлении киберпространством и говорить о каком-то независимом интернет-сообществе не приходится.

Учитывая сложность решаемых ICANN задач, свое функционирование оно осуществляет во взаимодействии со следующими структурами[1]: ASO (Address Supporting Organization) – организация поддержки адресов; ccNSO (Country Names Supporting Organisation) – организация поддержки национальных доменов; GNSO (Generic Names Supporting Organization) – организация поддержки доменов общего пользования; RSSAC (Root Server System Advisory Committee) – консультативный комитет системы корневых серверов; SSAC (Security and Stability Advisory Committee) – консультативный комитет по безопасности и стабильности; GAC (Government Advisory Committee) – правительственный консультационный комитет; ALAC (At-Large community) – консультативный комитет At-large.

Помимо этого, ICANN консультационно взаимодействует:

- с международным союзом электросвязи (International Telecommunication Union, ITU) – определяет стандарты в области телекоммуникаций;
- со всемирной организацией интеллектуальной собственности (Organisation Mondiale de la Properiete Intelectuelle, OMPI) – администрирование международных конвенций в области интеллектуальной собственности;
- с организацией экономического сотрудничества и развития (Organization for Economic Cooperation and Development, OECD) – международная экономическая организация развитых стран. Осуществляет аналитическую работу, вырабатывает рекомендации для стран-членов и служит платформой для организации многосторонних переговоров по экономическим проблемам.

Функционирование в контакте с этими организациями позволяет формировать и принимать в качестве рекомендаций «удобные» для ICANN стандарты, используемые протоколы, телекоммуникационное оборудование, определять порядок его функционирования и т.д. Все элементы телекоммуникационного оборудования и т.п. своевременно патентуются, что исключает возможность выхода на рынок «неугодных» производителей, а оставшихся производителей вынуждает покупать патенты. После чего все рекомендации, оборудование, протоколы и т.д. могут рекомендоваться посредством OECD как в странах, входящих его состав, так и мировому сообществу.

Региональные и локальные интернет регистраторы

Обеспечением технической составляющей функционирования киберпространства занимается RIR (Regional Internet Registrator) осуществляя: выделение IP-адресов, номеров автономных систем (Autonomous System, AS), мониторинг точек обмена трафиком, статистический анализ сетей, входящих в киберпространство и других технических сторон функционирования киберпространства. Все RIR коллективно образуют NRO (Number Resource Organization), созданную для представления интересов RIR и их глобального взаимодействия.

Статус RIR присваивается ICANN, а IANA выделяет объем ресурсов, которые RIR впоследствии будут делегировать своим членам. Перечень мировых RIR представлен в таблице 2.

Как видно из таблицы 2, на территории РФ как самих RIR, так и их представительств не имеется. На рис. 1 представлен граф связанности RIR.

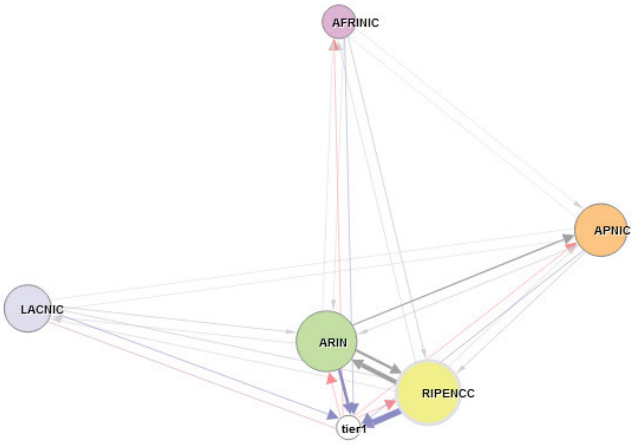

Рис. 1. Граф связанности региональных интернет-регистраторов (по данным ididb.ru)

Вершинами графа являются RIR, а ребрами количество соединений между ними, чем толще ребро между вершинами, тем больше соединений в нем проходит. Tier 1 – пиринговые операторы. Как видно из рисунка 1, наибольшее количество соединений имеется между Европой (в том числе Россией) RIPENCC, Северной Америкой (ARIN) и пиринговыми операторами, осуществляющими транзит трафика.

Каждый из RIR имеет автономные системы, расположенные в разных странах. Рассмотрим связанность RIR по странам, на рис. 2 представлен граф связанности AS по странам.

Вершины графа (рис. 2) – это страны. Чем больше в стране AS, тем она показана крупнее. Чем толще

1 Официальный сайт Internet Corporation for Assigned Names and Numbers. URL: https://www.icann.org/ (дата обращения 10.10.2021 г.)

Таблица 2

Перечень региональных интернет-регистраторов

RIR	Регион ответственности	Количество AS	Штаб-квартира
RIPE NCC	Европа, Центральная Азия и Ближний Восток	37191	Амстердам, Нидерланды
ARIN	Северная Америка и некоторые страны Карибского бассейна	30949	Вирджиния, США
APNIC	Восточная Азия и Тихоокеанский регион	23848	Брисбен, Австралия
LACNIC	Латинская Америка и большинство стран Карибского бассейна	12403	Монтевидео, Уругвай
AFRINIC	Африка	2033	Эбене, Маврикий

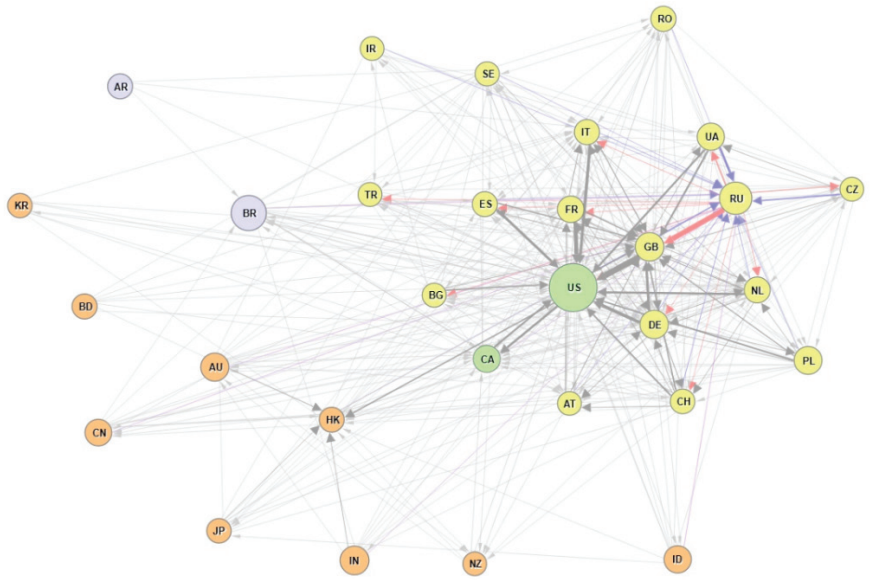

Рис. 2. Граф связанности AS по странам (по данным ididb.ru)

ребро графа, тем больше соединений между вершинами графа которые она соединяет.

Исходя из рис. 2 Российская Федерация наибольшее количество исходящих соединений имеет не со своими ближайшими соседями, а с Великобританией, а та в свою очередь с США, которая имеет максимальное количество связей из AS других стран. Такое количество связей с AS других стран позволяет утверждать, что первичная информация о функционировании киберпространства стекается в США, там агрегируется и обрабатывается. При этом, несмотря на проводимую в отношении РФ санкционную политику, наибольшее количество как исходящих, так и входящих соединений установлено со странами Запада.

В таблице 3 приведён список стран (ранжирован по количеству зарегистрированных AS) с указанием количества AS и задекларированных связей различного типа.

Исходя из таблицы 3, наибольшим количеством AS и связей с AS из других стран обладают США. В то же время в РФ практически в шесть раз меньше AS и связей с AS других стран по сравнению с США, однако количество исходящих соединений (UP-стримов) внутри страны превышает в четыре раза, а общая связанность в два раза аналогичные показатели США, что позволяет говорить о более высокой степени связанности киберпространства на территории РФ; при этом количество исходящих соединений к AS в других странах в РФ и США соизмеримы.

RIR осуществляют регистрацию LIR (Local Internet Registry) основная функция которых заключается в распределении и регистрации адресного простран-

Таблица 3

Список стран с указанием количества AS и задекларированных связей различного типа

№ п/п	Страна	Кол-во AS	Исходящих соединений к AS в других странах	Входящих соединений от AS из других стран	Всего связей с AS из других стран	Исходящих соединений внутри страны	Всего связей внутри страны
	США	28202	665	3792	15704	1797	5156
	Бразилия	8791	135	31	438	122	490
	Россия	5987	650	398	2667	7535	10158
	Индия	3208	25	4	53	1	12
	Великобритания	3003	913	1539	7540	656	2569
	Германия	2915	708	201	6969	1598	4642

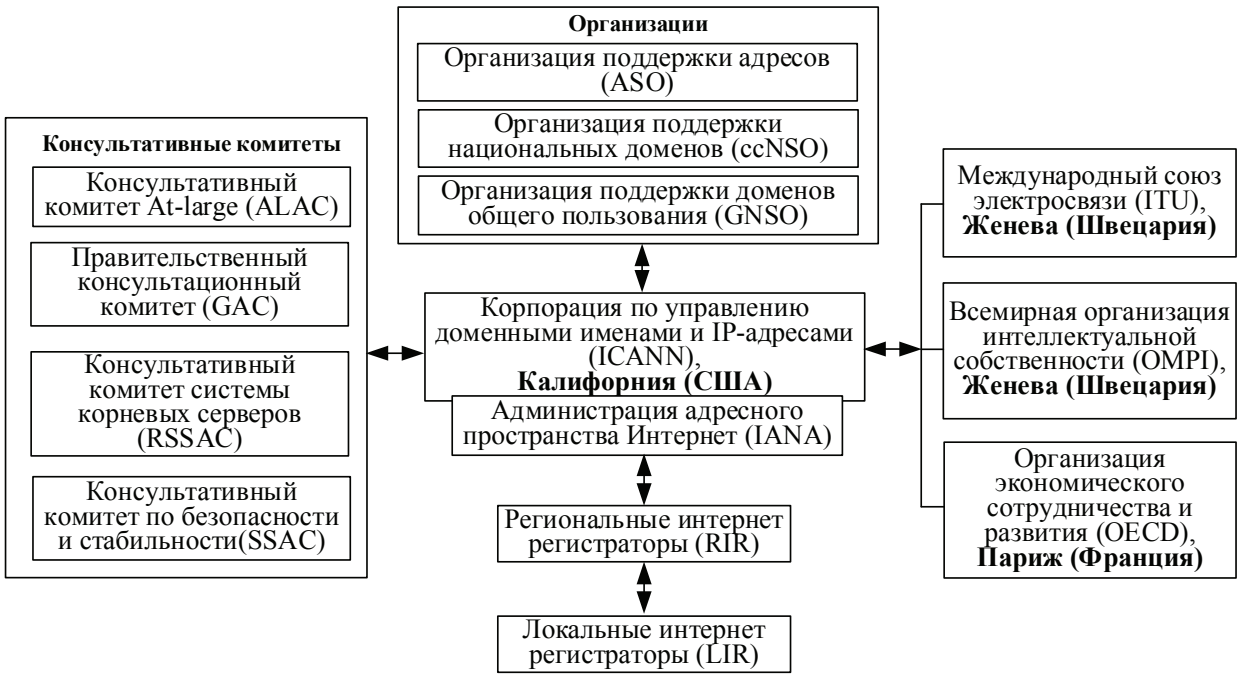

Рис. 3. Структура системы управления киберпространством (разработано автором)

ства на местных уровнях, утверждением локальных политик и процедур.

Таким образом, сложившуюся к настоящему времени организационную структуру системы управления киберпространством можно представить следующим образом (рис. 3).

Согласно теории систем данную структуру возможно детализировать на более низкие уровни, но для рассматриваемого в данном труде вопроса представленной детализации достаточно.

Автономные системы и точки обмена трафиком

Неоднократное упоминание AS требует их более подробного рассмотрения. Автономные системы являются одним из ключевых элементов в структуре киберпространства. Согласно международным рекомендациям[2], под автономной системой понимается совокупность маршрутизируемых диапазонов IP-адресов под единым административным управле-

2 RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS) URL: https://datatracker.ietf.org/doc/html/rfc1930 (дата обращения 10.10.2021 г.)

нием с общей, однозначно определённой политикой маршрутизации. Понятие «автономная система» относится не к физической, а к логической структуре сети, однако эта сущность оказывает определяющее влияние на весь процесс пересылки данных [21-23].

Каждая AS имеет уникальный номер и управляет как минимум одним диапазоном IP-адресов (IPv4, IPv6). Распределение IP-адресов регулируют RIR (LIR). Для обеспечения корректной маршрутизации трафика в сети, каждый владелец AS обязан оперативно вносить изменения в записи базы данных RIR (LIR), которые отражают политику маршрутизации.

Принадлежность AS к стране определяется на основе статистических отчетов RIR, которые, в свою очередь, отражают данные, предоставляемые компаниями в запросах на выделение ресурсов. В действительности, отдельно взятая AS может быть использована в стране, которая не была указана в запросе.

Регистрация AS может быть осуществлена RIR или LIR, для чего к ним необходимо отправить запрос с предоставлением: реквизитов организации; сведений о минимум двух AS готовых взаимодействовать с регистрируемой AS; обосновать необходимость запроса такого количества блоков IP-адресов; динамику использования предоставляемых IP-адресов в ближайшие два года; технические характеристики сети и оборудование, которое будет использоваться для обслуживания AS[3].

Предоставляемая по запросу RIR (или LIR) информация, несомненно, аккумулируется и подвергается дальнейшему анализу. Результатом анализа является многомерная «карта» всех мировых AS с указанием их связанности, технических характеристик, используемого оборудования, диапазонах IP-адресов, динамики активности на ближайшее время и т.д.

Эти данные достаточно полно характеризуют текущее состояние киберпространства, а также его прогнозные состояния с временным лагом в два года. Принципиально важно, что эти данные в полном объеме доступны киберкомандованиям иностранных государств, а регуляторам Российской Федерации в области телекоммуникаций они недоступны. Таким образом, отсутствуют объективные данные для управления ресурсами киберпространства, размещенными на территории РФ.

Рассмотрим вопрос связанности автономных систем на примере одной из крупнейших AS России – AS12389 (ПАО «Ростелеком»). На рисунках 4, 5, 6 представлена связанность AS12389 с другими AS и точками обмена трафиком.

Вершины MSK-IX(msk), MSK-IX(smr), MSK-IX(nsk), DATAIX (ua) – точки обмена трафиком, вершина 3491 – транзитная AS, а оставшиеся вершины – крупнейшие мировые операторы, ребра соединения по протоколу BGP (Border Gateway Protocol).

Связанность AS не является постоянной и изменяется в зависимости от интересов эксплуатирующей ее организации, технических причин и т.д., например, в период первой волны пандемии COVID-19 (когда большинство перешло на удаленную работу, или находились дома) граф внешней связанности автономной системы AS12389 (по состоянию на 30 марта 2020 года) выглядел иначе (рис. 6).

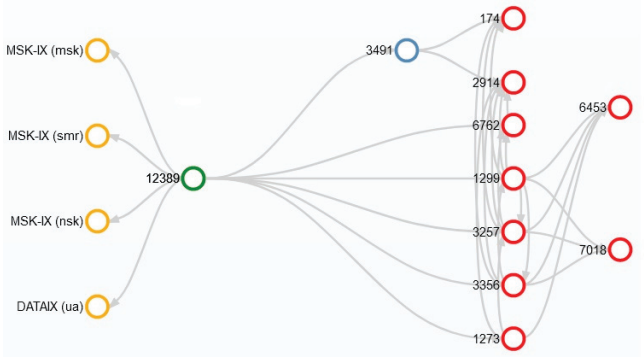

Рис. 4. Структура внешней связанности автономной системы AS12389 по состоянию на август 2021 года (по данным ididb.ru)

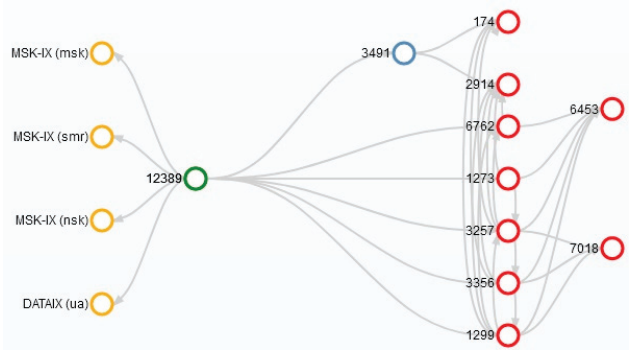

Рис. 5. Структура внешней связанности автономной системы по состоянию на сентябрь 2021 года (по данным ididb.ru)

Вершины MSK-IX(msk), MSK-IX(nsk), DATAIX (central), DATAIX (ua) – точки обмена трафиком. Вершины 199599, 3491, 5511, 51219, 31261, 31133 20485 – транзитные AS, а оставшиеся вершины – крупнейшие мировые операторы.

Таким образом, между собой AS могут связываться посредством точек обмена трафиком, транзитных AS и на прямую с другими AS (посредством протокола BGP). Связанность AS динамично изменяется во времени, не представляет особых технических сложностей и может быть изменена в любой момент в зависимости от потребностей организации эксплуатирующей AS или других AS с которыми осуществляется взаимодействие. Рассматривая все AS в совокупности, можно утверждать, что киберпространство динамично изменяет связанность (как логическую, так и физическую) во времени.

3 Что такое AS, кому и зачем она нужна. URL: https://tendence.ru/articles/autonomoussystem (дата обращения 10.10.2021 г.)

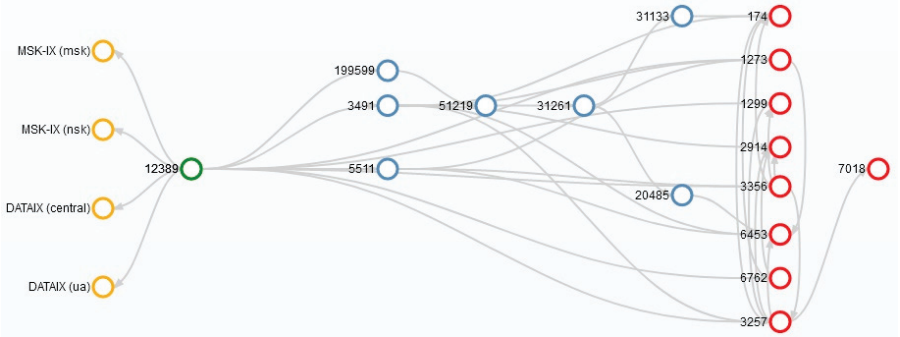

Рис. 6. Структура внешней связанности автономной системы AS12389 по состоянию на март 2020 года (по данным ididb.ru)

На первый взгляд, связанность изменяется в зависимости от нагрузки, количества предоставляемых услуг и их качества, перераспределения потоков данных и прохождение их по оптимальным маршрутам и т.д., однако основной целью операторов связи и транснациональных компаний, которым они принадлежат, является получение максимальной выгоды при минимальных затратах. Соответственно, все происходящие изменения структуры в первую очередь преследуют финансовую выгоду, а уже после этого – предоставление услуг потребителям, обеспечение заданного качества и т.д.

Под точкой обмена трафиком понимается сетевая инфраструктура, предназначенная для оперативной организации соединений и меж операторского обмена IP-трафика (пиринга) между независимыми сетями. Участниками обмена трафика являются организации, управляющие автономными системами. Точка обмена трафиком в большинстве случаев не является «точкой» в классическом ее понимании, а представляет собой совокупность технологических площадок в рамках города или страны, соединенных между собой высокоскоростными каналами передачи данных. Внутренняя структура точки обмена трафиком скрыта от участников обмена, поэтому для них она является «точкой».

Регуляторам Российской Федерации в области телекоммуникаций для осуществления эффективного управления Российским сегментом киберпространства необходимо собирать дополнительную информацию по структуре, местам расположения, аппаратной и программной составляющей, связанности, владельцам и т.д. точек обмена трафика. Регулятор должен видеть точки обмена трафика в виде полноценной инфраструктуры со всеми используемыми технологиями, протоколами и т.д.

Телекоммуникационные альянсы

Помимо описанных структур, значительное влияние на киберпространство оказывают телекоммуникационные операторы, которые управляют своими AS, принимают решения об изменении связанности с другими AS, добавляют новые линии и элементы киберпространства и т.д.. Координацию деятельности телекоммуникационных операторов осуществляют два крупных альянса – FreeMove и Bridje Alliance, охватывающих большую часть территории и населения нашей планеты.

Альянс **FreeMove**[4] был создан в 2003 году для предоставления международной связи. Включает в свой состав крупных Европейских телекоммуникационных операторов: Deutsche Telekom, TeliaSonera, Orange, Telecom Italia Group и Turkcell, которые являются лидерами рынка в Германии, Франции, Италии, Скандинавии и Балтийского региона, поддерживая более двух миллионов корпоративных мобильных соединений (порядка 60 – 65 % рынка) в пределах зоны Freemove.

FreeMove охватывает Западную и Восточную Европу, а также проходит по Азии, Северной и Южной Америке.

Помимо этого, FreeMove имеют стратегическое партнерство крупными операторами других стран: Cosmote group; Salt; T-Mobile US (США); Turkcell (Турция); Мегафон (Россия); Brige Alliance; Eircom; NOS и др.

Bridje Alliance – бизнес-альянс 36 крупных мобильных телекоммуникационных компаний Азиатско-Тихоокеанского региона, Ближнего Востока и Африки, обслуживающий порядка 900 млн. пользователей. Стратегические партнеры в Европе и Америке расширяют зону влияния альянса[5].

Концепция Bridje Alliance похожа на концепцию Европейского FreeMove, с которым она находится в партнерстве.

Таким образом, с первого взгляда независимые телекоммуникационные операторы принимают свои решения на основе координирующих органов (альянсов), которые, в первую очередь, действуют в своих интересах, и основной целью которых в мирное время является получение прибыли, и решения, принимаемые руководством альянса, оказывают влияние на деятельность операторов связи (непосредственно или косвенно). Фактически решения альянсов могут парализовать деятельность любого телекоммуникационного оператора.

Если решения ICANN и взаимосвязанных с ним структур оказывают влияние на RIR, LIR и AS в целом,

4 Официальный портал Freemove. URL: https://www.freemove.com/ (дата обращения 10.10.2021 г.)

5 Официальный портал Bridgealliance. URL: http://www.bridgealliance.com/ (дата обращения 10.10.2021 г.)

то решения телекоммуникационных альянсов оказывают влияние на AS, их связанность и политику внутри автономных систем, а также на получаемые конечными потребителями набор ресурсов и услуг (а также их стоимость), предоставляемых телекоммуникационными операторами.

Заключение

Управление киберпространством является крайне сложным процессом, задействующим множество структур, основной из которых является наднациональная структура ICANN, созданная и находящаяся в США, подчиненная их законодательству и действующая согласно модели управления, одобренной США. По факту управление киберпространством монополизировано ICANN и связанными с ней структурами.

В сложившихся условиях Российская Федерация фактически исключена (и продолжается процесс оттеснения) из процесса управления киберпространством, в том числе и на своей территории (как с географической точки зрения, так и с логической), а основные каналы управления и органы управления находятся за пределами РФ.

Регуляторы, крупнейшие потребители ресурсов и услуг киберпространства (в том числе силовые ведомства, элементы критической инфраструктуры и т.д.) лишены возможности управления Российским сегментом киберпространства и действуют на правах потребителей. При этом они обязаны предоставлять информацию, характеризующую состояние элементов киберпространства, целых сегментов (например, AS) зарубежным органам управления.

Российской Федерации необходимо осуществлять борьбу за управление киберпространством, причем как с точки зрения прибыли (если говорить о конкуренции телекоммуникационных операторов), так и с точки зрения национальной безопасности.

Рассмотренная структура управления киберпространством на данном уровне детализации позволила выделить следующие ключевые элементы киберпространства: корневые DNS сервера; хосты-реплики; автономные системы; точки обмена трафиком. Выделенные элементы в дальнейшем позволят проводить изучение киберпространства с последующей детализацией элементов.

Литература

1. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16-21.
2. Зарудницкий В.Б. Характер и содержание военных конфликтов в современных условиях и обозримой перспективе // Военная мысль. 2021. № 1. С.34-44.
3. Тумар В.А., Левчук Н.Н. Киберпространство как среда противоборства: военный аспект и Белорусский опыт нормотворчества // Вестник Академии военных наук. 2020. № 3 (72). С.43-49.
4. Дурнев Р.А., Крюков К.Ю., Дедученко Ф.М. Предупреждение техногенных катастроф, провоцируемых в ходе военных действий // Военная мысль. 2019. № 10. С. 41-48.
5. Жиленков А.А., Черный С.Г. Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 58-66. DOI:10.21681/2311-3456-2020-2-58-66.
6. Гущина Е.А., Макаренко Г.И., Сергин М.Ю. Обеспечение информационно-технологического суверенитета государства в условиях развития цифровой экономики // Право.by. 2018. № 6 (56). С. 59-63.
7. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии: Монография / Н.П. Ромашкина, А.С. Марков, Д.В. Стефанович. – Москва, 2020. Сер. Библиотека Национального исследовательского института мировой экономики и международных отношений имени Е.М. Примакова. – 98 с. ил.
8. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1(29). С. 2-8. DOI: 10.21681/2311-3456-2019-1-2-9.
9. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18-23. DOI: 10.21681/2311-3456-2019-3-18-23.
10. Добродеев А.Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2021. № 4 (44). С. 61-72 . DOI:10.21681/2311-3456-2021-4-61-72.
11. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Многовекторный конфликт в киберпространстве как предпосылка формирования нового вида Вооруженных Сил // Военная мысль. 2021. № 12. С.126-135.
12. Котенко И.В., Крибель А.М., Лаута О.С., Саенко И.Б. Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети // Электросвязь. 2020. № 12. С.54-59. DOI:10.34832/ELSV.2020.13.12.008.
13. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. 2021. № 1. С.36-44. DOI:10.34832/ELSV.2021.14.1.004
14. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. 2021. № 5 (45). С. 12-20. DOI:10.21681/2311-3456-2021-5-12-20.
15. Grechishnikov E.V., Dobryshin M.M., Kochedykov S.S., Novoselcev V.I. Algorithmic model of functioning of the system to detect and counter cyber-attacks on virtual private network // Journal of Physics: Conference Series. International Conference «Applied Mathematics, Computational Science and Mechanics: Current Problems», AMCSM 2018. 2019. С. 012064.

16. Бочков С.И., Макаренко Г.И., Федичев А.В. Об окинавской хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика. 2018. № 1. С. 4-14. DOI: 10.21681/1994-1404-2018-1-04-14
17. Starodubtsev Y.I., Balenko E.G., Zakalkin P.V., Fedorov V.H. Change dynamics for forms and opportunities of centers of power under globalization // В сборнике: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. С. 9271172. DOI: 10.1109/FarEastCon50210.2020.9271172.
18. Starodubtsev Y.I., Vershennik E.V., Balenko E.G., Fedorov V.H. Cyberspace: terminology, properties, problems of operation // В сборнике: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. С. 9271282. DOI: 10.1109/FarEastCon50210.2020.9271282.
19. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. № 4 (44). С. 16-24. DOI:10.21681/2311-3456-2021-4-16-24.
20. Закалкин П.В. Аспекты использования киберпространства в интересах корпоративных систем управления // Труды Научно-исследовательского института радио. 2021. № 4. С. 23-32.
21. Исследование структуры сети интернет: модели, инструменты, методики: монография / М.В. Иванов. – Орёл: Академия ФСО России, 2018. – 108 с. ил.
22. Иванов М.В., Калашников И.В., Нуруллаев М.М. Исследование структурных свойств сети интернет на основе метаграфовых моделей // Труды СПИИРАН. 2020. Т.19. № 4. С. 880-900.
23. Иванов М.В., Филимонов П.А. Модель сети Интернет на уровне автономных систем в виде безмасштабного графа // Телекоммуникации: Наука и технология. 2016. № 11. С. 22-26.

EVOLUTION OF CYBERSPACE MANAGEMENT SYSTEMS

***Zakalkin P. V.*[6]**

The purpose of the study: *to identify the main systems that control cyberspace and the key elements whose management will allow controlling a given segment of cyberspace.*

Research method: *theory of complex systems; synergetic.*

Result: *The paper considers the main control systems that play a key role in the management of cyberspace, highlights the structural elements of cyberspace and their interrelations with each other. Regional and local Internet registrars are considered, their coherence graph is presented, as well as the coherence graph by country. Based on the study, the author's vision of the organizational structure of the cyberspace management system (in relation to domain names and IP addresses). Autonomous systems and traffic exchange points are considered, the structure of external connectivity of autonomous systems and its change over time are given on examples. The largest telecommunication alliances are presented, which have an impact on the activities of telecom operators (directly or indirectly) and,* as a *result,* on the set of resources and *services (as well as their cost) received by end users provided by telecommunication operators.*

Scientific novelty: *the considered structure of the cyberspace management system made it possible to identify the main systems that control cyberspace and the key elements whose management will allow controlling a given segment of cyberspace.*

Keywords: *cyberspace, autonomous system, management, Internet registrars, traffic exchange point, telecommunication alliances, connectivity graph, ICANN.*

References

1. Starodubcev Yu.I., Zakalkin P.V., Ivanov S.A. Texnosfernaya vojna kak osnovnoj sposob razresheniya konfliktov v usloviyax globalizacii // Voennaya my'sl'. 2020. № 10. S.16-21.
2. Zarudnickij V.B. Xarakter i soderzhanie voenny'x konfliktov v sovremenny'x usloviyax i obozrimoj perspektive // Voennaya my'sl'. 2021. № 1. S.34-44.
3. Tumar V.A., Levchuk N.N. Kiberprostranstvo kak sreda protivoborstva: voenny'j aspekt i Belorusskij opy't normotvorchestva // Vestnik Akademii voenny'x nauk. 2020. № 3 (72). S.43-49.
4. Durnev R.A., Kryukov K.Yu., Deduchenko F.M. Preduprezhdenie texnogenny'x katastrof, provociruemy'x v xode voenny'x dejstvij // Voennaya my'sl'. 2019. № 10. S. 41-48.
5. Zhilenkov A.A., Cherny'j S.G. Sistema bezavarijnogo upravleniya kriticheski vazhny'mi ob"ektami v usloviyax kiberneticheskix atak // Voprosy' kiberbezopasnosti. 2020. № 2 (36). S. 58-66. DOI:10.21681/2311-3456-2020-2-58-66.

6 Pavel V. Zakalkin, Ph.D., doctoral candidate, Military Academy of Communications, St. Petersburg, Russia. E-mail: pzakalkin@mail.ru

6. Gushhina E.A., Makarenko G.I., Sergin M.Yu. Obespechenie informacionno-texnologicheskogo suvereniteta gosudarstva v usloviyax razvitiya cifrovoj e'konomiki // Pravo.by. 2018. № 6 (56). S. 59-63.
7. Romashkina N.P., Markov A.S., Stefanovich D.V. Mezhdunarodnaya bezopasnost', strategicheskaya stabil'nost' i informacionny'e texnologii: Monografiya / N.P. Romashkina, A.S. Markov, D.V. Stefanovich. – Moskva, 2020. Ser. Biblioteka Nacional'nogo issledovatel'skogo instituta mirovoj e'konomiki i mezhdunarodny'x otnoshenij imeni E.M. Primakova. – 98 s. il.
8. Romashkina N.P. Global'ny'e voenno-politicheskie problemy' mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy', perspektivy' // Voprosy' kiberbezopasnosti. 2019. № 1(29). S. 2-8. DOI: 10.21681/2311-3456-2019-1-2-9.
9. Karcxiya A.A., Makarenko G.I., Sergin M.Yu. Sovremenny'e trendy' kiberugroz i transformaciya ponyatiya kiberbezopasnosti v usloviyax cifrovizacii sistemy' prava // Voprosy' kiberbezopasnosti. 2019. № 3 (31). S. 18-23. DOI: 10.21681/2311-3456- 2019-3-18-23.
10. Dobrodeev A.Yu. Kiberbezopasnost' v Rossijskoj Federacii. Modny'j termin ili prioritetnoe texnologicheskoe napravlenie obespecheniya nacional'noj i mezhdunarodnoj bezopasnosti XXI veka // Voprosy' kiberbezopasnosti. 2021. № 4 (44). S. 61-72. DOI:10.21681/2311-3456-2021-4-61-72.
11. Starodubcev Yu.I., Zakalkin P.V., Ivanov S.A. Mnogovektorny'j konflikt v kiberprostranstve kak predposy'lka formirovaniya novogo vida Vooruzhenny'x Sil // Voennaya my'sl'. 2021. № 12. S.126-135.
12. Kotenko I.V., Kribel' A.M., Lauta O.S., Saenko I.B. Analiz processa samopodobiya setevogo trafika kak podxod k obnaruzheniyu kiberatak na komp'yuterny'e seti // E'lektrosvyaz'. 2020. № 12. S.54-59. DOI:10.34832/ELSV.2020.13.12.008.
13. Saenko I.B., Lauta O.S., Karpov M.A., Kribel' A.M. Model' ugroz resursam ITKS kak klyuchevomu aktivu kriticheski vazhnogo ob"ekta infrastruktury' // E'lektrosvyaz'. 2021. № 1. S.36-44. DOI:10.34832/ELSV.2021.14.1.004
14. Kondakov S.E., Rud' I.S. Model' processa provedeniya komp'yuterny'x atak s ispol'zovaniem special'ny'x informacionny'x vozdejstvij // Voprosy' kiberbezopasnosti. 2021. № 5 (45). S. 12-20. DOI:10.21681/2311-3456-2021-5-12-20.
15. Grechishnikov E.V., Dobryshin M.M., Kochedykov S.S., Novoselcev V.I. Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network // Journal of Physics: Conference Series. International Conference "Applied Mathematics, Computational Science and Mechanics: Current Problems", AMCSM 2018. 2019. S. 012064.
16. Bochkov S.I., Makarenko G.I., Fedichev A.V. Ob okinavskoj xartii global'nogo informacionnogo obshhestva i zadachax razvitiya rossijskix sistem kommunikacii // Pravovaya informatika. 2018. № 1. S. 4-14. DOI: 10.21681/1994-1404-2018-1-04-14
17. Starodubtsev Y.I., Balenko E.G., Zakalkin P.V., Fedorov V.H. Change dynamics for forms and opportunities of centers of power under globalization // V sbornike: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. S. 9271172. DOI: 10.1109/FarEastCon50210.2020.9271172.
18. Starodubtsev Y.I., Vershennik E.V., Balenko E.G., Fedorov V.H. Cyberspace: terminology, properties, problems of operation // V sbornike: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. S. 9271282. DOI: 10.1109/FarEastCon50210.2020.9271282.
19. Starodubcev Yu.I., Zakalkin P.V., Ivanov S.A. Strukturno-funkcional'naya model' kiberprostranstva // Voprosy' kiberbezopasnosti. 2021. № 4 (44). S. 16-24. DOI:10.21681/2311-3456-2021-4-16-24.
20. Zakalkin P.V. Aspekty ispol'zovanija kiberprostranstva v interesah korporativnyh system upravlenija // Trudy nauchno-issledovatel'skogo instituta radio. 2021. № 4. S. 23-32.
21. Issledovanie struktury' seti internet: modeli, instrumenty', metodiki: monografiya / M.V. Ivanov. – Oryol: Akademiya FSO Rossii, 2018. – 108 s. il.
22. Ivanov M.V., Kalashnikov I.V., Nurullaev M.M. Issledovanie strukturny'x svojstv seti internet na osnove metagrafovy'x modelej // Trudy' SPIIRAN. 2020. T.19. № 4. S. 880-900.
23. Ivanov M.V., Filimonov P.A. Model' seti Internet na urovne avtonomny'x sistem v vide bezmasshtabnogo grafa // Telekommunikacii: Nauka i texnologiya. 2016. № 11. S. 22-26.