# СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ КИБЕРПРОСТРАНСТВА

***Стародубцев Ю.И.[1], Закалкин П.В.[2], Иванов С.А.[3]***

***Цель исследования:*** *разработка структурно-функциональной модели киберпространства, как элемента его математической (аналитико-имитационной) модели, позволяющей исследовать свойства киберпространства. Формирование терминологического базиса исследуемой области.*

***Методы исследования:*** *теория сложных систем, синергетика.*

***Результат исследования:*** *разработана структурно-функциональная модель, описывающая процесс формирования информационных услуг на основе ресурсов киберпространства. Применительно к киберпространству введено понятие «симбионт» как универсальное понятие, позволяющее описать любой элемент киберпространства и его ресурсы. Даны определения терминам: киберпространство, информационный, вычислительный и телекоммуникационный ресурс. Помимо этого, представлена формализация ресурсов и информационных услуг, предоставляемых киберпространством. Показан пример формирования информационной услуги на основе ресурсов киберпространства.*

***Ключевые слова:*** *информационные услуги, информационные ресурсы, ресурсы киберпространства, формирование информационной услуги.*

**DOI:**10.21681/2311-3456-2021-4-16-24

## Введение

Процессы глобализации, развитие информационных и телекоммуникационных технологий предопределили незаметный для многих (но тем не менее стремительный) переход человечества в новую эпоху, в которой процессы коммуникации между искусственными и естественными участниками, их знания и опыт практически полностью перенесены в киберпространство.

Во второй половине 90-х годов прошлого столетия магистральные сети всех мировых операторов связи были объединены и интегрированы с вычислительными ресурсами, системами навигации, автоматизированными системами управления технологическими процессами. Это привело к появлению искусственного пространства планетарного масштаба – киберпространства, которое столь плотно вошло в симбиоз с привычным укладом жизни человечества, что зачастую кажется обыденным и вполне естественным [1-3]. Так, мы уже не представляем своей жизни без сотовых телефонов, банковских карт, систем навигации, Интернета и других устройств и услуг функционирующих посредством киберпространства.

Как показывает исторический опыт, человек всегда являясь источником конфликта, непременно порождает борьбу за обладание ресурсами. Киберпространство не стало исключением [4-6]. Опубликованные исследования показывают постоянный количественный и качественный рост кибервоздействий на критическую и корпоративную инфраструктуру различных государств[4] [7-10]. Это предопределяет необходимость изучения конфликтов, происходящих в киберпространстве.

Для понимания природы конфликта прежде всего необходимо описать его процесс, что осложняется рядом объективных причин:

- конфликт проходит в киберпространстве, которое в явном виде не определено и не формализовано, а его элементы не имеют однозначной государственной принадлежности. Это не позволяет построить строгую математическую модель пространства в котором протекает конфликт;
- характер конфликта неявен, но протекает в режиме реального времени;
- при однозначном установлении факта конфликта, нет его формализованного описания применительно к киберпространству, что не позволяет однозначно установить источник кибератак и задействованную при этом инфраструктуру киберпространства.

Для изучения конфликтов в киберпространстве, прежде всего необходимо изучить саму среду проведения конфликта, для чего в рамках данной статьи будет описана структурно-функциональная модель киберпространства.

---

1 Стародубцев Юрий Иванович, Заслуженный деятель науки РФ, доктор военных наук, профессор, профессор кафедры Военной академии связи, Санкт-Петербург, Россия. E-mail: prof.starodubtsev@gmail.com

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

3 Иванов Сергей Александрович, кандидат технических наук, докторант Военной академии связи, Санкт-Петербург, Россия. E-mail: sa-ivanov@mail.ru

4 1) Топ угроз ИБ в корпоративных сетях. Результаты мониторинга сетевого трафика в 2020 году // Positive Technologies. 2021. 9 с.
2) Кибербезопасность 2020-2021. Тренды и прогнозы // Positive Technologies. 2021. 25 с.

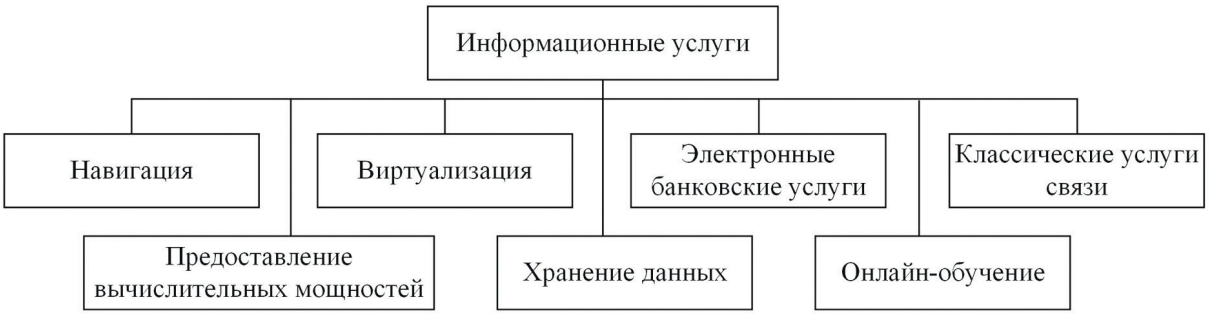


*Рис. 1. Информационные услуги, предоставляемые киберпространством*

**Структурные элементы киберпространства**

Прежде чем приступить к описанию структурно-функциональной модели киберпространства, необходимо определиться с понятием «киберпространство». В [2, 11] авторским коллективом обосновано и сформулировано следующее определение: *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.

Объективность существования киберпространства подтверждается множеством публикаций и международных нормативно-правовых документов[5] [12-15].

Объединение элементов киберпространства позволяет определить его физическую структуру. С функциональной точки зрения, элементами киберпространства, образующими его физическую структуру, являются:

1. Искусственная и естественная среда распространения сигналов;
2. Средства каналообразования;
3. Средства распределения ресурсов киберпространства (маршрутизаторы, коммутаторы и т.д.);
4. Средства измерения и сбора первичных характеристик элементов киберпространства и обрабатываемого трафика;
5. Вычислительные средства хранения и комплексной обработки первичных данных;
6. Средства разграничения и защиты информационных ресурсов (в том числе: средства аутентификации и идентификации);
7. Средства управления фрагментами киберпространства и (или) их функциями;
8. Средства хранения и обработки информационных ресурсов;
9. Автоматизированные источники и потребители информационных ресурсов (IoT, АСУ ТП, роботы и т.д.);
10. Средства определения навигационных данных;
11. Устройства коммуникационного сопряжения информационных потребностей человека и возможностей киберпространства.

Человек, на текущем этапе развития, в силу своих физиологических особенностей пока не может напрямую подключиться к киберпространству. Для получения доступа к ресурсам киберпространства и удовлетворения каких-либо своих потребностей человек вынужден использовать устройства ввода-вывода, которые позволяют преобразовать запрос человека в корректный, для восприятия киберпространством, вид.

Результатом объединения функциональных элементов киберпространства является реализация процессов обеспечения информационного обмена и формирования информационных услуг.

К процессам обеспечения информационного обмена относятся: маршрутизация, коммутация, обработка данных, каналообразование, передача данных, хранение данных, обеспечение безопасности (в том числе идентификация и аутентификация) и др. Помимо этого, объединение структурных элементов киберпространства позволяет формировать комплексные объекты, например линии и узлы связи.

Примеры информационных услуг, предоставляемых киберпространством представлены на рисунке 1.

**Симбионты киберпространства**

Все элементы киберпространства можно разбить на две основные группы устройств:

— устройства коммуникации, используемые человеком для удовлетворения своих нужд (смартфон, IoT-устройства, навигационное оборудование, станки с ЧПУ, «умные» производства (заводы) и т.д.);
— устройства, обеспечивающие готовность киберпространства к формированию и предоставлению запрашиваемых услуг (маршрутизаторы, ЦОД и т.д.).

Каждое из устройств потенциально обладает вычислительным ($Vr$), информационным ($Ir$) и телекомму-

5 1) ISO/EIC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity
2) The U.S. Army Concept for Cyberspace and Electronic Warfare Operations 2025-2040. TRADOC Pamphlet 525-8-6. January 2018. 38 p.
3) Cyberspace Operations. Joint Publication 3-12. 2018. 104 p.

никационным ресурсом ($Tr$). Помимо этого, человек, использующий элементы киберпространства, также обладает этими типами ресурсов:

- информационный ресурс человека – это его знания, мысли;
- вычислительный ресурс человека – мыслительные способности, посредством которых человек способен формировать новые знания. Фактически, вычислительный ресурс человека не изучен, но теоретически его способности безграничны;
- коммуникационный ресурс человека – способность передавать свои знания, мысли, эмоции и т.д. посредством слов, письма, жестов и т.д.

При подключении устройства к киберпространству оно становится его частью, соответственно и его ресурсы становится частью ресурса киберпространства. Процесс объединения ресурсов, фактически не зависит от желания конечного пользователя средства коммуникации. Примером являются *botnet* сети, в которые, без ведома конечного потребителя, объединяются устройства, подключенные к киберпространству[6].

Человек при использовании средств коммуникации также объединяет свои ресурсы с ресурсами киберпространства. Рассмотрим это на примере научной полемики на любом из форумов. Прочитав вопрос (потребив информационный ресурс), человек посредством мыслительных способностей (вычислительный ресурс) формирует на него ответ (информационный ресурс). Посредством коммуникационного устройства (например ноутбука) и своего коммуникационного ресурса сформированный ответ преобразуется в цифровой вид (посредством набора на клавиатуре ноутбука) и посредством телекоммуникационного оборудования передается на форум (информационный ресурс), тем самым пополняя информационный ресурс киберпространства.

Элементы киберпространства осуществляют информационный обмен не только в интересах человека, но и в интересах множества искусственных (небиологических) объектов (автоматизированные системы управления, системы мониторинга критической инфраструктуры, IoT, коммуникационное оборудование и т.д.), в разы превышающих количество биологических объектов (людей).

При этом, при отсутствии доступа к киберпространству многие устройства, использующие его ресурсы, существенно снижают свои функциональные возможности, вплоть до полного отсутствия функционала (например, система навигации в автомобиле, распределенная АСУ, маршрутизаторы и т.д.). Реализация полного функционала каждого из устройств зависит от возможности обеспечения его доступа к ресурсам киберпространства.

Таким образом, каждый элемент киберпространства:

- помимо потребления ресурсов киберпространства, дополняет его своими ресурсами;
- может быть небиологическим объектом (устройством) или биологическим (человеком, являющимся одновременно творцом киберпространства);
- без доступа к ресурсам киберпространства снижает свои функциональные возможности, вплоть до полного отсутствия функционала.

Необходимо отметить, что, с одной стороны, на первоначальном этапе формирования киберпространства Человек являлся исключительно его разработчиком и создателем, а, с другой стороны, на современном этапе в определенных аспектах жизнедеятельности Человек стал элементом киберпространства, продолжая при этом его развивать.

Являясь высокотехнологичной средой, киберпространство изменило подход к определению потребителя (применительно к киберпространству), а существующая терминология, описывающая понятие «потребитель» и «пользователь»[7] не позволяет отобразить процессы, происходящие в киберпространстве в исходном смысле этих понятий. Эти факторы требуют введение нового термина, позволяющего описать взаимоотношения между элементами киберпространства.

Проведя параллель с животным миром, взаимоотношения между элементами киберпространства можно характеризовать как мутуалистический облигатный симбиоз, характеризующийся тем, что взаимодействия между организмами выгодны друг другу (в нашем случае – взаимодействие как между техническими системами, так и между техническими системами и Человеком). На основании этого, авторским коллективом применительно к киберпространству предлагается вместо терминов «потребитель» и «пользователь» использовать термин «симбионт».

Предлагается следующая классификация симбионтов:

- *внешние симбионты* (по отношению к киберпространству) – симбионты, которые в любой произвольный момент времени могут подключиться (или отключиться) к киберпространству для обеспечения доступа к его ресурсам. К данному типу симбионтов можно отнести смартфоны, персональные компьютеры, системы навигации, IoT-устройства, АСУ ТП и т.д.
- *внутренние симбионты* (по отношению к киберпространству) – симбионты, обеспечивающие функционирование киберпространства. Примером могут служить маршрутизаторы, ЦОД, базовые станции сетей подвижной связи и т.д. – другими словами телекоммуникационное оборудование операторов, связи, составляющее основу их сетей.

6 1)Информационная безопасность интернета вещей [Электронный ресурс] URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернета_вещей_(Internet_of_Things)
2) Positive Research 2019 Сборник исследований по практической безопасности 2019 // Positive Technologies. С. 297.
3) Positive Research 2020 Сборник исследований по практической безопасности 2020 // Positive Technologies. С. 274.

7 1) ГОСТ Р ИСО/МЭК 12207—99. Государственный стандарт Российской Федерации: «Процессы жизненного цикла программных средств».
2) ГОСТ 34.003—90. Государственный стандарт Российской Федерации: «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
3) Закон РФ от 07.02.1992 N 2300-1 (ред. от 22.12.2020) «О защите прав потребителей».

Учитывая, что каждое из устройств, являющееся элементом киберпространства, потенциально обладает вычислительным ($Vr$), информационным ($Ir$) и телекоммуникационным ресурсом ($Tr$), соответственно, согласно теории сложных систем, и киберпространство обладает вычислительным, информационным и телекоммуникационным ресурсом.

В первую очередь необходимо рассмотреть информационные ресурсы. В научно-методической литературе[8], [16-17] приводятся различные классификации информационных ресурсов, основными недостатками которых являются: фактическое отсутствие учета материальности ресурсов, а также факторов их влияния на киберпространство. Авторским коллективом предлагаются следующие классификации информационных ресурсов:

*1. По способу представления:*

— хранимые на носителях информации (электронные и традиционные носители информации);
— находящиеся в киберпространстве (хранимые, передаваемые, обрабатываемые и т.д.);
— формируемые на основе знаний. Для человека данный вид информационных ресурсов представлен в виде знаний и мыслей, для устройств – в виде алгоритмов функционирования, порядков обработки данных и т.д., сформированных в результате мыслительного процесса человека.

*2. По способу использования:*

— служебные. Информационные ресурсы используемые для осуществления взаимодействия между элементами киберпространства (маршрутно-адресные таблицы, служебная информация передаваемая при установлении соединения и т.д.);
— знания. Совокупность структурированных и неструктурированных данных, а также формализованные способы и методы их упорядоченной обработки, позволяющие формировать новые знания в соответствии с запросом симбионта.

Телекоммуникационные и вычислительные ресурсы рассматривались в различных публикациях [12, 18], поэтому в рамках данной статьи более подробно останавливаться на них не будем.

Информационные услуги, предоставляемые киберпространством формируются автоматически по запросу симбионта посредством упорядоченного объединения ресурсов киберпространства согласно правил формирования услуги.

На рисунке 2 представлено графическое отображение взаимосвязи ресурсов и услуг киберпространства.


*Рис. 2. Графическое отображение взаимосвязи ресурсов и услуг киберпространства*

Исходя из этого, возникает необходимость корректировки определений существующих терминов: информационная услуга, вычислительный ресурс, телекоммуникационный ресурс, информационный ресурс. Авторским коллективом сформулированы следующие определения:

*Информационная услуга* – услуга, сформированная в результате функционирования киберпространства в ответ на запрос симбионта.

*Вычислительный ресурс* – совокупность объединенных ресурсов, предназначенных для формирования и предоставления запрашиваемых симбионтами информационных услуг.

*Телекоммуникационный ресурс* – взаимосвязанная совокупность частотных, энергетических, канальных, коммутационных и др. ресурсов, предназначенных для обеспечения удаленного доступа симбионтов к информационным услугам.

*Информационный ресурс* – совокупность структурированных и неструктурированных данных, упорядоченная обработка которых позволяет сформировать информационные услуги по запросу различных симбионтов.

**Формализованное представление ресурсов киберпространства**

В общем случае, ресурс киберпространства ($R_{КП}$) можно представить следующим образом:

$$R_{КП} = f\left(R_{КП}^{Ir}, R_{КП}^{Vr}, R_{КП}^{Tr}\right)$$

где

$R_{КП}^{Ir}$ – информационный ресурс киберпространства;

$R_{КП}^{Vr}$ – вычислительный ресурс киберпространства;

$R_{КП}^{Tr}$ – телекоммуникационный ресурс киберпространства.

Однако, ресурс киберпространства динамически изменяется во времени за счет постоянного изменения количества симбионтов (внутренних и внешних). При этом, внутренние симбионты составляют основное ядро киберпространства и в бесконечно малый период времени ресурс ядра киберпространства (без учета внешних симбионтов) можно представить как:

8 1) ГОСТ Р 53622-2009, Информационные технологии (ИТ). Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность документов. Введен в действие 01.01.2011. – М.: Стандартинформ, 2011, 12 с.
2) ГОСТ Р 43.0.2-2006 Информационное обеспечение техники и операторской деятельности. Термины и определения. Введен в действие 01.07.2007. М.: Издательство стандартов, 2007, 7 с.
3) Ковалева Н.Н. Правовая природа государственных информационных ресурсов // Информационные ресурсы России. М., 2012. № 2. С. 24–27.

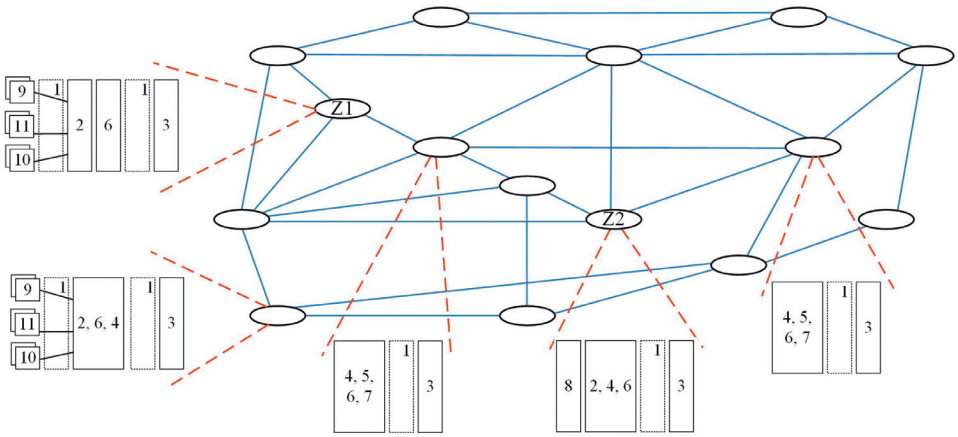


*Рис. 3. Графическое отображение примера объединения функций элементов киберпространства*

$$R_{\text{ЯКП}} = f\left(\sum_{i=1}^{I} R_i^{\text{ВС}}\right)$$

где

$R_i^{BC}$ – ресурс i-го внутреннего симбионта киберпространства;

$I$ – количество внутренних симбионтов.

Внешний симбионт с помощью телекоммуникационного оборудования, посредством точки доступа подключается к ресурсам киберпространства созданного другими симбионтами. Подключившись к киберпространству и став его частью, внешний симбионт изменит объем ресурсов киберпространства. Таким образом, общий ресурс киберпространства в условиях подключения к нему внешних симбионтов (в бесконечно малый период времени) можно представить следующим образом:

$$R_{\text{КП}} = f\left(\sum_{i=1}^{I} R_i^{\text{ВС}} + \sum_{l=1}^{L} R_l^{\text{ВНС}}\right)$$

где

$R_l^{\text{ВНС}}$ – ресурс *l*-го внешнего симбионта киберпространства;

$L$ – количество внешних симбионтов подключенных к киберпространству.

Ресурс, добавляемый (убавляемый) симбионтом, подключившемуся к киберпространству, можно представить следующим образом:

$$\Delta = R^{\text{с}}_{\text{общ}} - R_{\text{собств}} - R_{\text{ВЗ}}$$

где $\Delta$ – объем добавляемого (убавляемого) ресурса киберпространства;

$R^{\text{с}}_{\text{общ}}$ – общий ресурс симбионта, подключенного к киберпространству;

$R_{\text{собств}}$ – ресурс, затрачиваемый на собственное функционирование элемента (операционная система, прикладное ПО и т.д.);

$R_{\text{ВЗ}}$ – ресурс, затрачиваемый на взаимодействие с ресурсами КП.

Каждый из ресурсов $R^{\text{с}}_{\text{общ}}$, $R_{\text{собств}}$ и $R_{\text{вз}}$ представляет собой совокупность информационных, телекоммуникационных и вычислительных ресурсов.

**Функциональное представление формирования информационной услуги, предоставляемой киберпространством**

Рассмотрим пример объединения функций элементов киберпространства, позволяющих, в конечном итоге, сформировать информационную услугу, предоставляемую симбионту (рисунок 3).

Симбионт, используя вычислительные, информационные и телекоммуникационные ресурсы устройства ввода-вывода и преобразования информации (например, смартфон (блок 11, рис. 4), осуществляет запрос на получение информационной услуги (например, удаленный доступ к корпоративной базе данных (блок 8, рис. 4). В случае со смартфоном запрос передается по радио каналу (среда распространения сигнала (блок 1, рис. 4) до каналообразующего оборудования базовой станции оператора связи (блок 2, рис. 4). Запрос посредством вычислительных, информационных и телекоммуникационных ресурсов, базовой станции обрабатывается и передается на систему обнаружения атак (или МЭ), основной функцией которых является обеспечение безопасности (блок 6, рис. 4). Далее запрос попадает на маршрутизатор (блок 3, рис. 4), обрабатывается и передается по маршруту до получателя, где попадает на систему обнаружения атак (или МЭ) и в конечном итоге достигает распределенной базы данных.

Серверная платформа, где размещена база данных, посредством своего телекоммуникационного оборудования обрабатывает запрос, осуществляет идентификацию и аутентификацию симбионта, осуществившего запрос. Осуществляет разрешение доступа потребителя к хранимым данным и формирует ответ на запрос симбионта. После чего, посредством телекоммуникационного оборудования ответ на запрос передается симбионту в виде информационной услуги.

Однако не стоит рассматривать информационную услугу как совокупность функций нескольких устройств. Информационная услуга может оказываться и в рамках одного устройства (рис. 4).

Рассмотрим эту процедуру на примере маршрутизатора. Получив входные данные, маршрутизатор посредством своего телекоммуникационного оборудования

обрабатывает их, при этом обращаясь к динамической таблице маршрутизации (информационный ресурс) и вычислительному ресурсу (например, использование центрального процесса для обработки запроса). Основываясь на данных, полученных из таблицы маршрутизации, маршрутизатор формирует маршрут и посредством своего телекоммуникационного оборудования передает данные следующему устройству маршрутизации (коммутации) в сети связи.


*Рис. 4. Графическое отображение примера формирования информационной услуги в рамках одного устройства*

Получение данных из таблицы маршрутизации и внесение данных в нее, использование процесса при осуществлении этой процедуры и при расчете маршрута являются для маршрутизатора информационными услугами, формируемыми собственными информационными, вычислительными и телекоммуникационными ресурсами маршрутизатора.

**Формализованное представление информационных услуг, формируемых киберпространством**

Оборудование, подключенное к точке доступа, становится своеобразным «окном» к ресурсам киберпространства с помощью которого симбионт может получать информационные услуги. Для формирования *m*-ой услуги ($IU_m$) симбионт формирует запрос, который обрабатывается элементами киберпространства. Для формирования $IU_m$ используется *m*-ая часть информационного, вычислительного и телекоммуникационного ресурсов киберпространства на основе которых посредством правил формирования услуги ($Z_m$) формируется запрашиваемая симбионтом услуга.

В зависимости от времени, местоположения, характера нагрузки на ресурсы киберпространства, одна и та же услуга, формируемая по одному и тому же правилу, по запросу одного того же симбионта, может задействовать ресурсы киберпространства в различных долях, пропорциях, и физически относящихся к различным элементам киберпространства. Примером может служить территориальное перемещение симбионта, в процессе которого изменяется точка доступа к ресурсам киберпространства (смартфон автоматически сменяет используемые им базовые станции, смена точек доступа Wi-Fi и т.д.). Смена точки доступа приводит к изменению маршрутов передачи трафика внутри киберпространства и, как следствие, к количественному изменению используемых для формирования услуги ресурсов.

Информационная услуга, предоставляемая киберпространством формируется на основе ресурсов киберпространства согласно правил формирования услуги. В формализованном виде информационная услуга ($IU$) может быть представлена как:

$$IU_m = f\left(R^{Ir}_{m\text{КП}}, R^{Vr}_{m\text{КП}}, R^{Tr}_{m\text{КП}}, Z_i\right)$$

где

$Z_m$ – правило формирования *m*-ой услуги,

$R^{Ir}_{m\text{КП}}$ – информационный ресурс киберпространства затрачиваемый на формирование *m*-ой услуги,

$R^{Vr}_{m\text{КП}}$ – вычислительный ресурс киберпространства затрачиваемый на формирование *m*-ой услуги,

$R^{Tr}_{m\text{КП}}$ – телекоммуникационный ресурс киберпространства затрачиваемый на формирование *m*-ой услуги.

Из всего множества информационных услуг, предоставляемых киберпространством, *i*-ому симбионту будет предоставлен набор, ограниченный его запросом ($Zapros$) и возможностями ($Vozm$), оборудования подключаемого к точке доступа. Набор информационных услуг, предоставляемых киберпространством симбионту ($IU_{\text{симбионт}}$), можно представить как:
$IU_{\text{симбионт}} = f\left(Zapros, Vozm\right)$ при этом $IU_{\text{симбионт}} \in IU_{\text{кп}}$
где $IU_{\text{кп}}$ – множество информационных услуг предоставляемых киберпространством.

Исходя из этого, графическое отображение структурно-функциональной модели киберпространства можно представить следующим образом (рисунок 5).

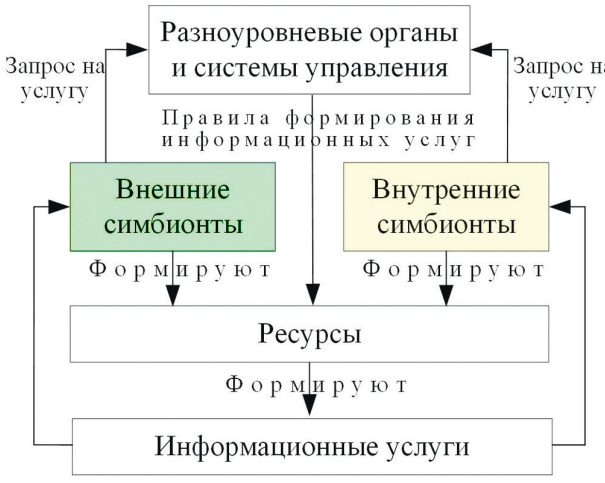


*Рис. 5. Графическое отображение структурно-функциональной модели киберпространства*

DOI:10.21681/2311-3456-2021-4-16-24

### Материальность ресурсов и информационных услуг киберпространства

В процессе формирования каждого из ресурсов киберпространства затрачиваются:

- *энергетические ресурсы* (необходимы для энергообеспечения элементов киберпространства);
- *кадровые ресурсы* (создание, эксплуатация, обслуживание технической и программной составляющей элементов киберпространства);
- *финансовые ресурсы* (оплата труда обслуживающего персонала, затрачиваемой элементами киберпространства энергии, закупка программной и технической составляющей и т.д.);
- *временные ресурсы* (формирование и предоставление ресурса требует временных затрат, помимо этого временной ресурс расходуется на обслуживание элементов киберпространства т.д.).
- *интеллектуальные ресурсы* (формирование теории, правил комплексирования ресурсов для получения требуемого результата).

Исходя из этого, в формализованном виде каждый из ресурсов ( $R$ ) киберпространства может быть представлен как функция:

$$R = f\left(E, Ch, F, T, In\right)$$

где $E$ – энергетический ресурс; $Ch$ – кадровый ресурс; $F$ – финансовый ресурс; $T$ – временной ресурс; $In$ – интеллектуальный ресурс.

Таким образом, на формирование каждого из ресурсов киберпространства затрачиваются материальные ресурсы, поэтому в соответствии с законом сохранения энергии можно говорить о том, что каждый из ресурсов киберпространства ($Vr$, $Ir$, $Tr$) является **материальным**.

На основе того, что каждая информационная услуга, предоставляемая киберпространством формируется посредством всех видов его материальных ресурсов, в соответствии с законом сохранения энергии можно утверждать о том, что и информационная услуга **материальна**. Таким образом, киберпространство состоит из материальных ресурсов и формирует материальные услуги по запросу симбионтов, что еще раз подтверждает материальность исследуемого пространства – киберпространства.

### Выводы

1. Структурно-функциональная модель является основой для создания аналитико-имитационных моделей киберпространства.
2. Необходимость разработки аналитико-имитационной модели обуславливается следующими задачами:
   - количественная оценка роста и распределения информационных ресурсов по элементам киберпространства;
   - исследование закономерностей изменения неоднородностей киберпространства;
   - формирование данных для оптимизации процессов управления ресурсами киберпространства;
   - анализ свойств киберпространства для формирования требований к элементам и разработки алгоритмов их функционирования.

**Достоверность исследования** подтверждается:

- использованием апробированных исходных данных, характеризующих параметры киберпространства;
- наличием и учетом отечественных и международных нормативных документов, регламентирующих процессы функционирования киберпространства;
- использованием ключевых положений теории сложных систем;
- статистическими данными по количественным и качественным характеристикам оконечных устройств, подключающихся к киберпространству.

### Литература


1. 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. DOI: 10.1109/FarEastCon50210.2020.9271282.
2. 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.
3. Дурнев Р.А., К.Ю. Крюков, Дедученко Ф.М. Предупреждение техногенных катастроф, провоцируемых в ходе военных действий // Военная мысль. 2019. № 10. С. 41–48.
4. Дылевский И.Н., Базылев С.И., Запивахин О.В., Комов С.А. и др. О взглядах администрации США на киберпространство как новую сферу ведения военных действий // Военная мысль. 2020. № 10. С. 22–29.
5. 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.
6. 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.
7. 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.
8. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография // Университет Иннополис. Иннополис: Издательский дом «Афина», 2017. 440 с.

9. Ревенков П.В., Бердюгин А.А., Макеев П.В. Оценка риска нарушения кибербезопасности в коммерческом банке (на примере атак на банкоматы “brute force” и “black box”) // Вопросы кибербезопасности. 2021. № 3 (43). С. 20–30. DOI:10.21681/2311-3456-2021-3-20-30.
10. 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.
11. Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации // Военная мысль. 2021. № 4. С. 39–49.
12. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. СПб.: Наукоемкие технологии, 2020. 337 с.
13. Шнепс-Шнеппе М.А., Селезнев С.П., Намиот Д.Е., Куприяновский В.П. О кибербезопасности критической инфраструктуры государства // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 7. 2016. С.22–31.
14. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского Университета. Серия 18. Социология и политология. 2018. Т. 24. № 1. С. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70.
15. Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261–269.
16. Стародубцев Ю.И., Давлятова М.А. Экономика цифровых информационных ресурсов // Санкт-Петербургский политехнический университет Петра Великого. Санкт-Петербург, 2019.
17. Оленичев М.Е., Чулюков В.А. Основы классификации цифровых информационных ресурсов // В сборнике: Информационные технологии в образовательном процессе вуза и школы Материалы XIII Всероссийской научно-практической конференции. 2019. С. 97–100.
18. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. СПб.: Наукоемкие технологии, 2017. 546 с.

# STRUCTURAL AND FUNCTIONAL MODEL OF CYBERSPACE

***Starodubtsev Yu. I.[9], Zakalkin P. V.[10], Ivanov S. A.[11]***

***Abstract. The aim of the research*** *is to develop a structural and functional model of cyberspace as an element of its mathematical (analytical and simulation) model, which allows us to study the properties of cyberspace. Formation of the terminological basis of the research area.*

***Research methods:*** *theory of complex systems, synergetics.*

***Research result:*** *a structural and functional model has been developed that describes the process of forming information services based on cyberspace resources. In relation to cyberspace, the concept of “symbiont” is introduced as a universal concept that allows describing any element of cyberspace and its resources. The following terms are defined: cyberspace, information, computing and telecommunications resource. In addition, the formalization of resources and information services provided by cyberspace is presented. An example of forming an information service based on cyberspace resources is shown.*

***Keywords:*** *information services, information resources, cyberspace resources, information service formation.*

## References

1. 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. DOI: 10.1109/FarEastCon50210.2020.9271282.
2. Starodubtcev Iu.I., Zakalkin P.V., Ivanov S.A. Tekhnosfernaia voi`na kak osnovnoi` sposob razresheniia konfliktov v usloviiakh globalizatcii // Voennaia my`sl`. 2020. № 10. S.16–21.
3. Durnev R.A., K.Iu. Kriukov, Deduchenko F.M. Preduprezhdenie tekhnogenny`kh katastrof, provotciruemy`kh v hode voenny`kh dei`stvii` // Voennaia my`sl`. 2019. № 10. S. 41–48.
4. Dy`levskii` I.N., Bazy`lev S.I., Zapivahin O.V., Komov S.A. i dr. O vzgliadakh administratcii SSHA na kiberprostranstvo kak novuiu sferu vedeniia voenny`kh dei`stvii` // Voennaia my`sl`. 2020. № 10. S. 22–29.

9 Yuri Starodubtsev, Honored Scientist of the Russian Federation, Dr.Sc., Professor, Professor of the Department, Military Academy of Communications, St. Petersburg, Russia. E -mail: prof.starodubtsev@gmail.com

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

11 Sergey Ivanov, Ph.D., doctoral candidate, Military Academy of Communications, St. Petersburg, Russia. E-mail: sa-ivanov@mail.ru

5. Romashkina N.P. Global`ny`e voenno-politicheskie problemy` mezhdunarodnoi` informatcionnoi` bezopasnosti: tendentcii, ugrozy`, perspektivy` // Voprosy` kiberbezopasnosti. 2019. № 1(29). S. 2–8. DOI: 10.21681/2311-3456-2019-1-2-9.
6. 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.
7. Zhilenkov A.A., Cherny`i` S.G. Sistema bezavarii`nogo upravleniia kriticheski vazhny`mi ob``ektami v usloviiakh kiberneticheskikh atak // Voprosy` kiberbezopasnosti. 2020. № 2 (36). S. 58–66. DOI:10.21681/2311-3456-2020-2-58-66.
8. Petrenko S.A., Stupin D.D. Natcional`naia sistema rannego preduprezhdeniia o komp`iuternom napadenii: nauchnaia monografiia // Universitet Innopolis. Innopolis: Izdatel`skii` dom «Afina», 2017. 440 s.
9. Revenkov P.V., Berdiugin A.A., Makeev P.V. Ocenka riska narusheniia kiberbezopasnosti v kommercheskom banke (na primere atak na bankomaty` “brute force” i “black box”) // Voprosy` kiberbezopasnosti. 2021. № 3 (43). S. 20–30. DOI:10.21681/2311-3456-2021-3-20-30.
10. Kartchiia A.A., Makarenko G.I., Sergin M.Iu. Sovremenny`e trendy` kiberugroz i transformatciia poniatiia kiberbezopasnosti v usloviiakh tcifrovizatcii sistemy` prava // Voprosy` kiberbezopasnosti. 2019. № 3 (31). S. 18–23. DOI: 10.21681/2311-3456- 2019-3-18-23.
11. Starodubtcev Iu.I., Ivanov S.A., Zakalkin P.V. Kontceptual`ny`e napravleniia resheniia problemy` obespecheniia ustoi`chivosti Edinoi` seti e`lektrosviazi Rossii`skoi` Federatcii // Voennaia my`sl`. 2021. № 4. S. 39–49.
12. Makarenko S.I. Modeli sistemy` sviazi v usloviiakh prednamerenny`kh destabiliziruiushchikh vozdei`stvii` i vedeniia razvedki. Monografiia. SPb.: Naukoemkie tekhnologii, 2020. 337 s.
13. Shneps-Shneppe M.A., Seleznev S.P., Namiot D.E., Coopriianovskii` V.P. O kiberbezopasnosti kriticheskoi` infrastruktury` gosudarstva // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 7. 2016. S.22–31.
14. Dobrinskaia D.E. Kiberprostranstvo: territoriia sovremennoi` zhizni // Vestneyk Moskovskogo Universiteta. Seriia 18. Sotciologiia i politologiia. 2018. T. 24. № 1. S. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70.
15. Danel`ian A.A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva // Obrazovanie i pravo. 2020. № 1. S. 261–269.
16. Starodubtcev Iu.I., Davliatova M.A. E`konomika tcifrovy`kh informatcionny`kh resursov // Sankt-Peterburgskii` politekhnicheskii` universitet Petra Velikogo. Sankt-Peterburg, 2019.
17. Olenichev M.E., Chuliukov V.A. Osnovy` classifikatcii tcifrovy`kh informatcionny`kh resursov // V sbornike: Informatcionny`e tekhnologii v obrazovatel`nom protcesse vuza i shkoly` Materialy` KHIII Vserossii`skoi` nauchno-prakticheskoi` konferentcii. 2019. S. 97–100.
18. Makarenko S.I. Informatcionnoe protivoborstvo i radioe`lektronnaia bor`ba v setecentricheskikh voi`nakh nachala XXI veka. Monografiia. SPb.: Naukoemkie tekhnologii, 2017. 546 s.