СТРУКТУРНО-ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ КОНФЛИКТНОЙ СИТУАЦИИ МЕЖДУ ГОСУДАРСТВЕННОЙ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНОСТРАННОЙ СИСТЕМОЙ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Стародубцев Ю. И.[1], Закалкин П. В.[2]

DOI: 10.21681/2311-3456-2024-4-82-91

Цель исследования: *определить взаимосвязь понятий «информационная инфраструктура» Российской Федерации и «киберпространство»; определить предпосылки реализации возрастающего множества деструктивных воздействий.*

Методы исследования: *системный анализ, классификация, сравнительный анализ.*

Полученные результаты: *рассмотрена система обеспечения информационной безопасности Российской Федерации, ее участники, информационная инфраструктура Российской Федерации и определена ее взаимосвязь с киберпространством. Осуществлена формализация рассмотренных элементов. Разработано графическое отображение взаимосвязи информационной инфраструктуры и киберпространства.*

Научная новизна: *Осуществлен системно-структурный анализ конфликтной ситуации, что позволило выявить объективные причины реализации множества деструктивных воздействий на объекты критической инфраструктуры.*

Ключевые слова: *киберпространство, информационная безопасность, информационная инфраструктура, атака, деструктивные воздействия.*

STRUCTURAL AND FUNCTIONAL ANALYSIS OF THE CONFLICT SITUATION BETWEEN THE STATE INFORMATION SECURITY SYSTEM AND A FOREIGN SYSTEM OF DESTRUCTIVE INFLUENCES

Starodubtsev Yu. I.[3], Zakalkin P. V.[4]

The purpose of the study: *to determine the relationship between the concepts of «information infrastructure» of the Russian Federation and «cyberspace»; to determine the prerequisites for the implementation of an increasing set of destructive influences.*

Research methods: *system analysis, classification, comparative analysis.*

The results obtained: *the information security system of the Russian Federation, its participants, the information infrastructure of the Russian Federation are considered and its relationship with cyberspace is determined. The formalization of the considered elements has been carried out. A graphical representation of the relationship between information infrastructure and cyberspace has been developed.*

Scientific novelty: *A system-structural analysis of the conflict situation has been carried out, which made it possible to identify the objective reasons for the implementation of many destructive effects on critical infrastructure facilities.*

Keywords: *cyberspace, information security, information infrastructure, attack, destructive effects.*

1 Стародубцев Юрий Иванович, Заслуженный деятель науки РФ, Заслуженный изобретатель РФ, доктор военных наук, профессор, профессор кафедры, Военная академия связи, Санкт Петербург, Россия. E-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476

2 Закалкин Павел Владимирович, кандидат технических наук, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

3 Yuri Starodubtsev, Honored Scientist of the Russian Federation, Honored Inventor of the Russian Federation, Doctor of Military Sciences, Professor, Professor of the Department, Military Academy of Communications, Saint Petersburg, Russia. E-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476

4 Pavel Zakalkin, Ph.D., Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

Введение

Сложнейшая военно-политическая обстановка в мире привела к началу Специальной военной операции и, как следствие, к переформатированию мирового порядка. Одним из отличительных факторов данного военного конфликта является кардинально возросшая роль киберпространства при ведении военных действий. Резко возросло количество кибератак, осуществляемых противоборствующими сторонами (как открыто, так и посредством своих «прокси» группировок), появились новейшие вооружения, навигация и управление которыми осуществляется посредством киберпространства.

Исходя из новых реалий глава военного комитета НАТО адмирал Роб Бауэр заявил, что «Кибератака на одну из стран НАТО может стать поводом для применения 5-й статьи устава Североатлантического альянса»[5]. Признавая киберпространство как пространство ведения военных действий, НАТО готово в любой момент (руководствуясь своими интересами) объявить Российской Федерации войну исходя только из факта наличия атак, осуществляемых посредством киберпространства.

Рассмотрев основные руководящие документы, имеющие отношение как к военной безопасности страны, так и к информационной безопасности, было установлено, что на законодательном уровне в Российской Федерации понятие «киберпространство» не определено.

Согласно Доктрины информационной безопасности Российской Федерации[6] (далее – Доктрина) в основном используются термины «информационная инфраструктура Российской Федерации»[7], «информационная сфера»[8] и «информационное пространство». Т.е. сложилась парадоксальная ситуация, НАТО готово объявить Российской Федерации войну в киберпространстве (попутно создавая киберкомандования в странах участницах альянса), осуществляет множество скоординированных кибератак на инфраструктуру РФ, а в РФ само понятие «киберпространство» не определено.

Данное исследование в первую очередь направлено на определение взаимосвязи понятий «информационная инфраструктура Российской Федерации», «информационная сфера» и «киберпространство».

Система обеспечения информационной безопасности

На государственном уровне в Доктрине признается, что:

- противник пытается доминировать в информационном пространстве за счет технологического превосходства и повсеместного внедрения иностранного оборудования, протоколов и т.д.;
- невозможно реализовать совместное справедливое, основанное на принципах доверия, управление этим пространством (даже хотя бы на территории собственного государства);
- отсутствуют международно-правовые нормы, регулирующие межгосударственные отношения в этом пространстве.

Согласно Доктрины обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации[9] (КИИ) и ЕСЭ РФ, в мирное время, в период непосредственной угрозы агрессии и в военное время является национальным интересом РФ в информационной сфере. В Доктрине определяется система обеспечения информационной безопасности[10] (СОИБ). С технической точки зрения СОИБ включает подсистемы контроля, принятия решений и формирования управляющих воздействий. При этом все подсистемы функционируют на ограниченном множестве учитываемых параметров.

В графическом виде СОИБ в РФ представлена на рисунке 1.

Система обеспечения информационной безопасности

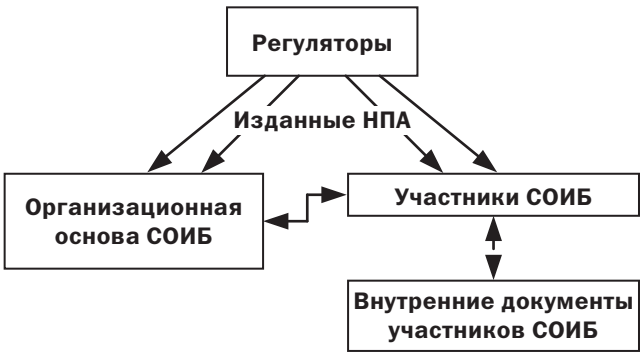

Рис. 1. Обобщенная структура системы обеспечения информационной безопасности в РФ

5 Кибератака может стать поводом для применения пятой статьи устава НАТО [Электронный ресурс] URL: https://rg.ru/2024/06/01/nato-mozhet-ispolzovat-5-iu-statiu-ustava-iz-za-kiberataki-na-strany-aliansa.html

6 Доктрина информационной безопасности российской Федерации. Утверждена Указом Президента Российской Федерации от 05.12.2016 г.

7 Информационная инфраструктура Российской Федерации – совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

8 Информационная сфера – совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

9 Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

10 Система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

В структуре СОИБ выделяются три основных элемента: регуляторы, организационная основа СОИБ и участники СОИБ.

В РФ имеется два основных регулятора в области информационной безопасности: ФСБ и ФСТЭК. Их задачи представлены в соответствующих руководящих документах[11].

Все элементы СОИБ РФ руководствуются нормативно-правовыми актами (НПА), издаваемыми регуляторами, и используют программные и программно-аппаратные средства, лицензированные ими.

СОИБ является частью системы обеспечения национальной безопасности Российской Федерации. Обеспечение ИБ осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

СОИБ должна строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Согласно Доктрины организационная основа СОИБ состоит из элементов, представленных на рисунке 2.

11 1) Федеральный закон от 3 апреля 1995 г. N 40-ФЗ «О федеральной службе безопасности».
2) Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.11.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

Согласно Доктрины участники СОИБ РФ представлены на рисунке 3.

Министерства и ведомства имеют право на создание собственных внутренних документов применительно к ИБ в части их касающихся. Получается, что в РФ имеется множество участников СОИБ, в процессе своей деятельности руководствующихся НПА, изданными регуляторами, и в дополнение к этому частично использующих внутренние документы.

В формализованном виде СОИБ можно представить следующим образом:

$$\{\{NPA^{R}\},\{Org\},\{Uch\},\{NPA^{Uch}\}\} = СОИБ$$

где $\{NPA^{R}\}$ – множество НПА, изданных регуляторами; $\{Org\}$ – множество элементов, составляющих организационную основу СОИБ; $\{Uch\}$ – множество участников СОИБ; $\{NPA^{Uch}\}$ – множество внутренних документов участников СОИБ.

Вся совокупность выделенных элементов: множество НПА, изданных регуляторами, множество элементов, составляющих организационную основу СОИБ, множество участников СОИБ и множество внутренних документов участников СОИБ – направлена на обеспечение ИБ информационной инфраструктуры РФ.

Структурное представление системы обеспечения информационной безопасности

Рассмотрим СОИБ со стороны участника СОИБ. Исходя из представленных выше документов каждый из участников СОИБ может руководствоваться НПА как одного из регуляторов, так и нескольких сразу и еще при этом иметь внутреннюю документацию применительно к ИБ. Также каждый из участников СОИБ

Организационная основа СОИБ РФ

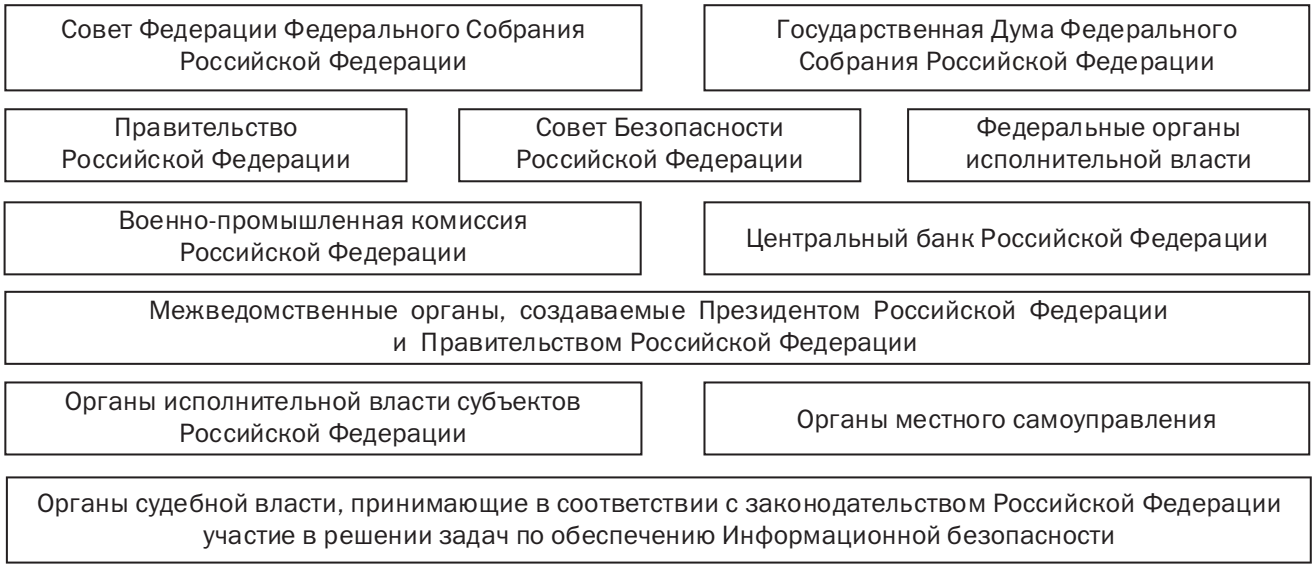

Рис. 2. Организационная основа СОИБ РФ

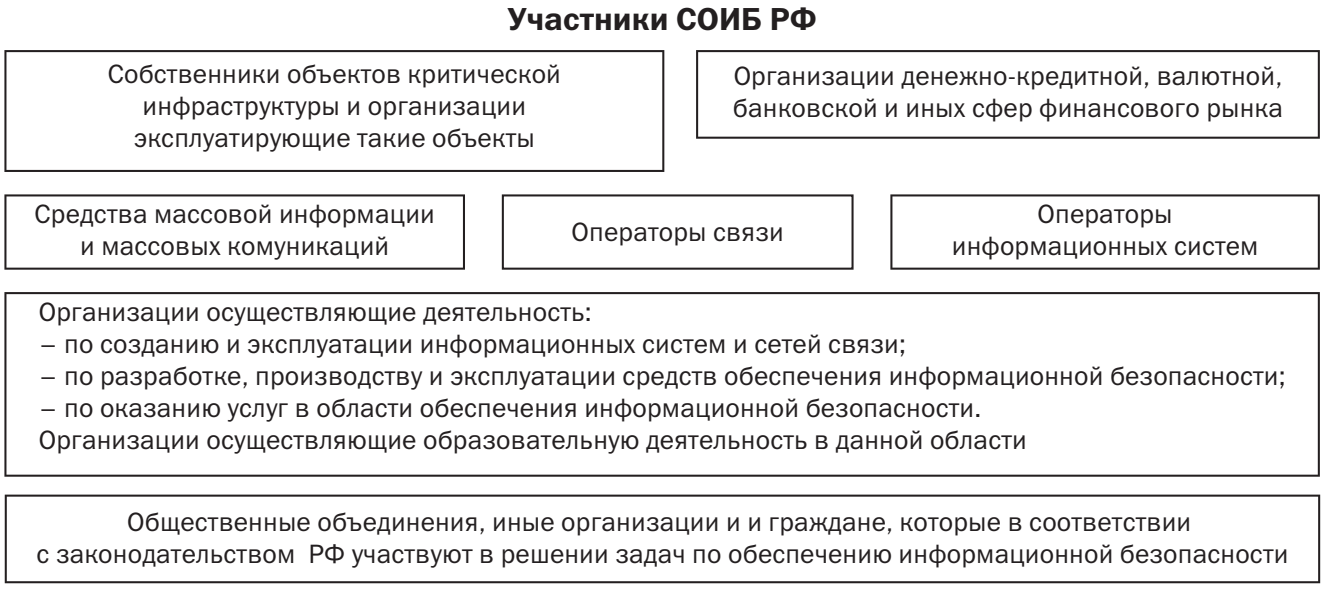

Рис. 3. Участники СОИБ РФ

в рамках своей ответственности может иметь несколько элементов информационной инфраструктуры.

В качестве примера сложившейся ситуации приведен рисунок 4. Участник СОИБ ($Uch1$) руководствуется НПА регулятора NPA^{R1} и собственной внутренней документацией применительно к ИБ (NPA^{Uch1}), имеет в зоне своей ответственности некоторое множество элементов информационной инфраструктуры Ii_1^{Uch1}, Ii_2^{Uch1}, Ii_n^{Uch1} (где n – количество элементов информационной инфраструктуры $Uch1$). При этом ответственным за элементы информационной инфраструктуры участника СОИБ может назначаться как одно лицо, так и несколько лиц, все зависит от территориальной рассосредоточенности структурных элементов участника СОИБ. Например, практически все органы государственной власти на территории РФ имеют деление, условно повторяющее административно-территориальное деление РФ. Соответственно лица ответственные за элементы информационной инфраструктуры Дальневосточного ФО и Центрального ФО будут различны.

В тоже время $Uch2$ может руководствоваться как NPA^{R1}, NPA^{R2}, так и собственной внутренней документацией применительно к ИБ (NPA^{Uch2}). Например, ФСТЭК для ряда своих НПА указывает что их действие не распространяется на высшие органы государственной власти и т.д., в таком случае используются НПА другого регулятора. $Uch2$ имеет собственное множество элементов информационной инфраструктуры Ii_1^{Uch2}, Ii_2^{Uch2}, Ii_k^{ch2} (где k – количество элементов информационной инфраструктуры NPA^{lsp}) и множество лиц, ответственных за ее эксплуатацию.

Исходя из приведенного графического представления видно, что каждый из участников СОИБ

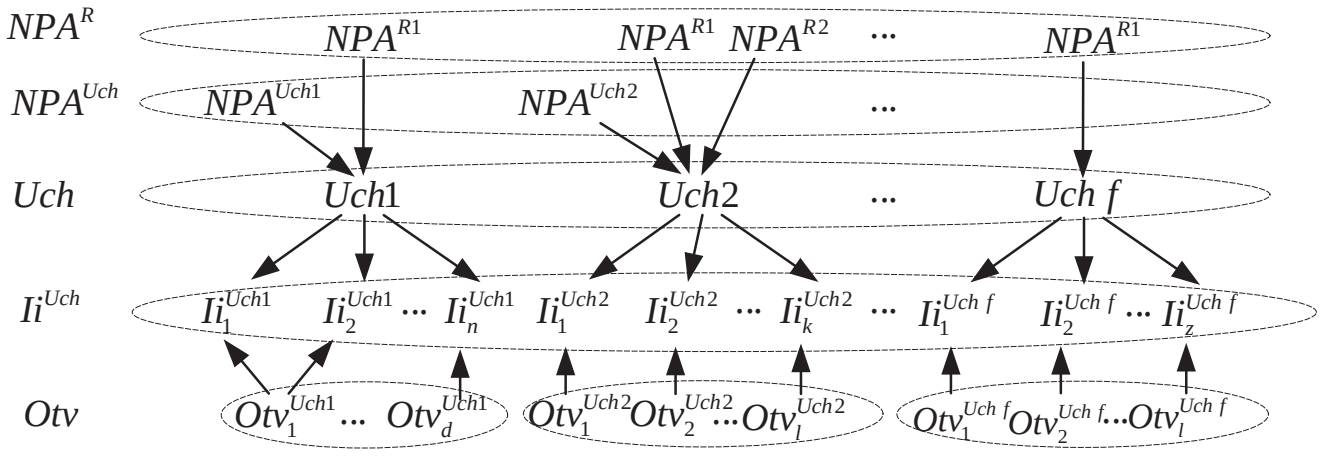

Рис. 4. Графическое представление взаимосвязи элементов СОИБ

применительно к своей инфраструктуре использует подмножество НПА (NPA^{Isp}) из общего множества НПА регуляторов, внутреннюю документацию применительно к ИБ, и при всем этом у участников имеется произвольный набор элементов информационной инфраструктуры и лиц, ответственных за обеспечение ее эксплуатации.

В формализованном виде участника СОИБ можно представить следующим образом:

$$Uch2 = \{NPA^{Isp}_{Uch2}, Ii^{Uch2}, Otv^{Uch2}\}$$

где $NPA^{Isp}_{Uch2} = \{NPA^{R1}_{Uch2}, NPA^{R2}_{Uch2}, NPA^{Uch2}\}$, при $NPA^{R1} \notin NPA^{R2}$, $NPA^{R1}_{Uch2} \cap NPA^{R1}$, $NPA^{R2}_{Uch2} \cap NPA^{R2}$; $Ii^{Uch2} = \{Ii^{Uch2}_1, Ii^{Uch2}_2, ..., Ii^{ch2}_k\}$, k – количество элементов информационной инфраструктуры; $Otv^{Uch2} = \{Otv^{Uch2}_1, Otv^{Uch2}_2, ..., Otv^{ch2}_l\}$, l – количество лиц, ответственных за функционирование информационной инфраструктуры $Uch2$.

Каждый из участников СОИБ действует в рамках НПА, изданных регуляторами, но при этом в первую очередь участник заинтересован в обеспечении безопасного функционирования собственной информационной инфраструктуры. Например, оператор связи заинтересован в безопасном функционировании элементов информационной инфраструктуры, находящейся в его ведении, но при этом функционирование инфраструктуры других операторов связи ему интересно только в рамках варианта обеспечения транзита собственного трафика через них.

Таким образом, вся информационная инфраструктура РФ не равноценно разделена между участниками СОИБ, за обеспечение ее функционирования отвечает множество лиц с различной степенью компетенции и различными техническими возможностями по обеспечению функционирования инфраструктуры.

Если вся информационная инфраструктура РФ функционирует в рамках СОИБ РФ, где определены регуляторы, организационная основа, участники, ответственные лица и т.д., вся инфраструктура защищена согласно требованиям, то возникает логичный вопрос «Откуда появляется противник, осуществляющий атаки на инфраструктуру?».

Для ответа на этот вопрос необходимо вернуться к определению термина «информационная инфраструктура», исходя из которого видно, что информационная инфраструктура РФ ограничивается только территорией РФ, а также территориями, находящимися под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации. При этом абсолютно не учитывается инфраструктура зарубежных государств.

Физическая составляющая информационной инфраструктуры РФ имеет множество точек взаимодействия с инфраструктурой зарубежных государств,

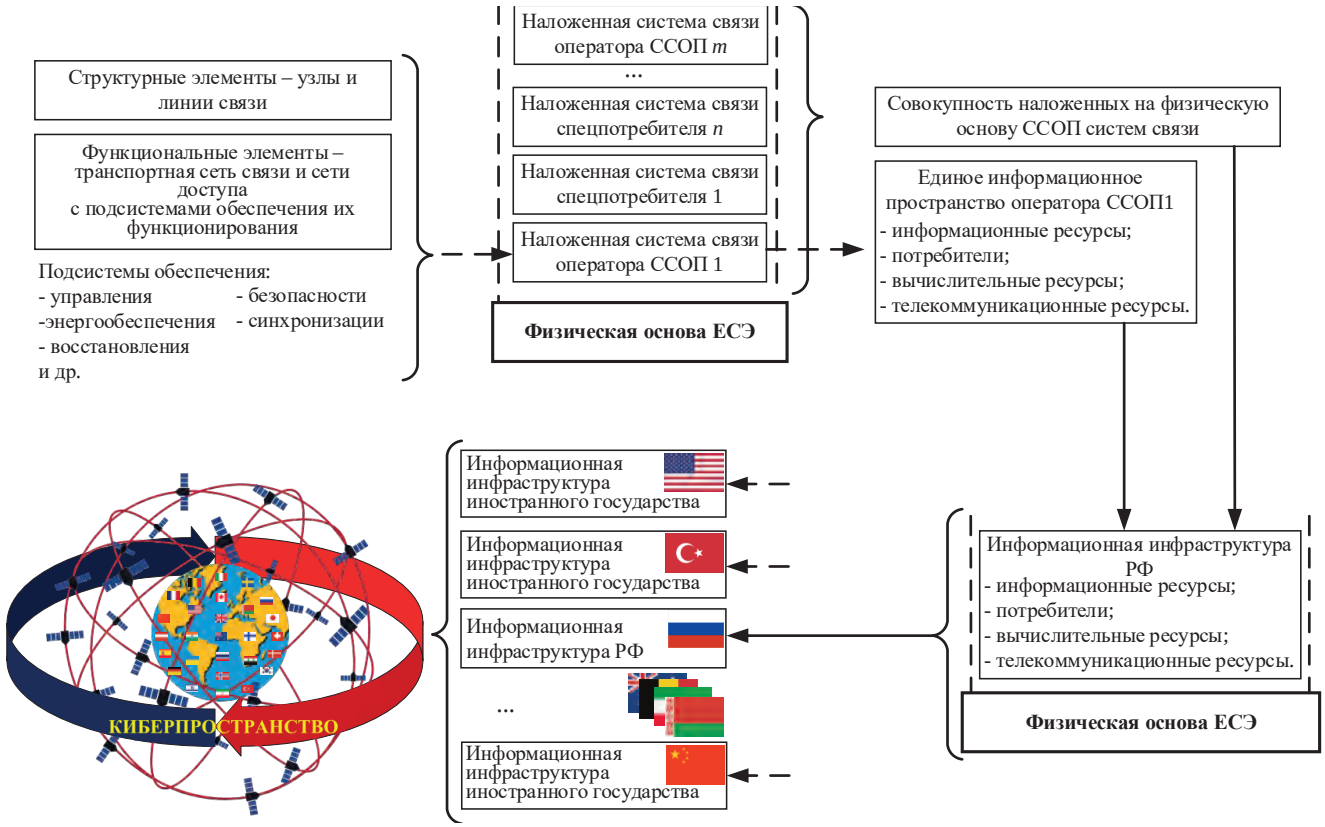

Рис. 5. Графическое отображение взаимосвязи понятий «информационная инфраструктура» и «киберпространство»

тем самым интегрируясь в одно глобальное пространство мирового масштаба, которое с различной степенью плотности покрывает все пространство нашей планеты. Поверх физической составляющей наложено множество логических структур. Графическое отображение этой ситуации представлено на рисунке 5. Наличие большого количества слабоконтролируемых связей (а также использование зарубежного оборудования, протоколов и т.д.) с инфраструктурой иностранных государств позволяет осуществлять деструктивные воздействия на информационную инфраструктуру РФ из любой точки земного шара [1–4], а заблаговременно внедренные программные закладки и зарубежное программное обеспечение облегчают эту задачу [5-6].

Взаимодействие с инфраструктурой иностранных государств является критичным для РФ, т.к. частично функционирование элементов информационной инфраструктуры возможно только в совокупности с этим пространством, и отдельно без него существенно ограничивается функционал или полностью прекращается его работа. Например, корневые сервера, отвечающие за адресацию, корневые DNS сервера и т.д. полностью контролируются зарубежными организациями [1].

Если распространить терминологию, применяемую в РФ на весь мир, то получается, что каждое государство имеет свою информационную инфраструктуру, имеющую точки взаимодействия с инфраструктурой других государств (как минимум соседних). В формализованном виде это можно представить следующим образом:

$$Ii^{MIR} = \{Ii^{RF}, Ii_1^{ig}, Ii_2^{ig}, Ii_3^{ig},..., Ii_z^{ig}\}$$

где Ii^{MIR} – общемировая информационная инфраструктура; z – общее количество мировых государств.

Терминология, принятая в различных государствах, в той или иной степени отличается, но в подавляющем большинстве общемировую информационную инфраструктуру называют киберпространством. Получается, что информационная инфраструктура РФ является составляющей киберпространства. Говоря о киберпространстве, мы подразумеваем и информационную инфраструктуру РФ (как составляющую киберпространства), а говоря о информационной инфраструктуре РФ мы подразумеваем киберпространство (как общее пространство, включающее в себя информационную инфраструктуру РФ).

Исходя из этого определение термина «информационная инфраструктура» требует корректировки. Предлагается под информационной инфраструктурой РФ понимать территориально выделенный структурный элемент киберпространства, представляющий собой взаимосвязанную совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Мировые информационные инфраструктуры не являются единственными составляющими киберпространства, в [1,2] указывается, что элементами киберпространства являются также и симбионты киберпространства. Т.е. устройства, которые в любой произвольный момент времени могут подключиться (или отключиться) к киберпространству для обеспечения доступа к его ресурсам и реализации отдельных системных функций в интересах других пользователей информационных услуг. К симбионтам можно отнести смартфоны, персональные компьютеры, системы навигации, IoT-устройства, АСУ ТП и т.д.

Информационная инфраструктура как элемент киберпространства

Киберпространство можно представить в виде множества, включающего в себя множество подмножеств, каждое из которых в свою очередь также состоит из множества подмножеств. Например, представив киберпространство как множество Ii^{MIR}, подмножествами данного множества будет множество информационных инфраструктур Ii^{mg} мировых государств. Каждое из множеств является множеством подмножеств, включающих в себя элементы, составляющие физическую и логическую структуру киберпространства. Которые в свою очередь включают в себя подмножества из множества участников СОИБ, организационной структуры, ответственных лиц, а также множества симбионтов в динамике, подключающихся (отключающихся) к элементам киберпространства.

При этом всякое объединение подмножеств будет являться частью подмножеств Ii^{mg}, также как и всякое пересечение всякого конечного семейства множеств из Ii^{mg} будет множеством из Ii^{mg}.

Учитывая, что физические элементы киберпространства покрывают всю поверхность нашей планеты (с различной степенью плотности) [1,2,7], а наша планета в приближенном виде имеет форму шара (обычно для описания фигуры Земли используют эллипсоид вращения или геоид), то киберпространство можно представить в виде шара. Физические элементы киберпространства могут находиться как в ближнем космосе (спутники), так и на морском дне (подводные коммуникационные кабели), то логичнее говорить о форме киберпространства, как о сферической оболочке (или сферическом слое) – области, заключенной между двумя концентрическими сферами различного радиуса.

Исходя из общей топологии[12] можно утверждать, что киберпространство является топологической структурой. Топологической структурой в множестве X называют структуру, образованную заданием множества Ω подмножеств множества X, обладающего следующими свойствами:

- всякое объединение множеств из Ω есть множество из Ω;
- пересечение всякого конечного семейства множеств из Ω есть множество из Ω.

Множества Ω называются открытыми множествами топологической структуры, определяемой посредством Ω в X.

Раз киберпространство наделено топологической структурой, следовательно, согласно общей топологии, оно является топологическим пространством.

В данном случае мы говорим только о физической структуре киберпространства, логическая структура является гораздо более сложной и многомерной, где на одном физическом элементе может пересекаться множество логических.

Киберпространство взаимоувязано и из любой его точки можно попасть в любую другую, что позволяет осуществлять атаки на элементы киберпространства (в нашем случае информационная инфраструктура), не находясь в непосредственной близости от них.

Предположим, что из информационной инфраструктуры иностранного государства (Ii^{ig}) осуществляется атака ($attack$) на элементы информационной инфраструктуры РФ (Ii^{RF}), например на элементы участников $Ii^{Uch1} = \{Ii_1^{Uch1}, Ii_3^{Uch1}\}$, $Ii^{Uch2} = \{Ii_2^{Uch2}, Ii_3^{Uch2}\}$ и $Ii^{Uch3} = \{Ii_1^{Uch3}, Ii_3^{Uch3}\}$ (Рисунок 6).

$$attack = \{aIi_1^{Uch1}, aIi_3^{Uch1}, aIi_2^{Uch2}, aIi_3^{Uch2}, aIi_1^{Uch3}, aIi_3^{Uch3}\}$$

12 Н. Бурбаки Общая топология. Основные структуры. М., 1968 г. 272 стр. с илл.

где aIi – атакованная информационная инфраструктура.

Далее необходимо ввести ограничения касаемо лиц, ответственных за элементы информационной инфраструктуры:

- ответственные лица с помощью имеющихся в их распоряжении технических средств (либо другим способами) получили уведомление об атаке на находящиеся в их ведении инфраструктуры;
- обладают высоким уровнем профессиональных компетенций, доверены, имеют в своем распоряжении достаточное количество технических средств и осведомлены о тактиках и техниках как проведения атак, так и противодействия им.

В связи с этим, далее будем считать $Otv^{Uch} = const$.

Авторский коллектив прекрасно понимает, что в реальной жизни у всех Otv^{Uch} будет различный уровень подготовки, технических и финансовых возможностей. Кроме того, во многих случаях атака может быть не зафиксирована, поскольку в системах защиты отсутствуют необходимые правила детектирования, учитывающие актуальные изменения в ландшафте киберугроз [8–10].

В данном примере целенаправленно показывается идеальный случай, когда все обнаружено и имеется достаточный ресурс для противодействия атаке.

Каждый из ответственных лиц из общего количества атакованной инфраструктуры будет видеть только атаки на инфраструктуру, за которую он ответственен, либо в отдельных случаях атаки на инфраструктуру участника СОИБ, которому он подчиняется. В этом случае общая информированность ответственного лица Inf^{Otv} будет определяться как:

$$Inf^{Otv} = \frac{ali_{vid}^{Otv}}{ali_n}$$

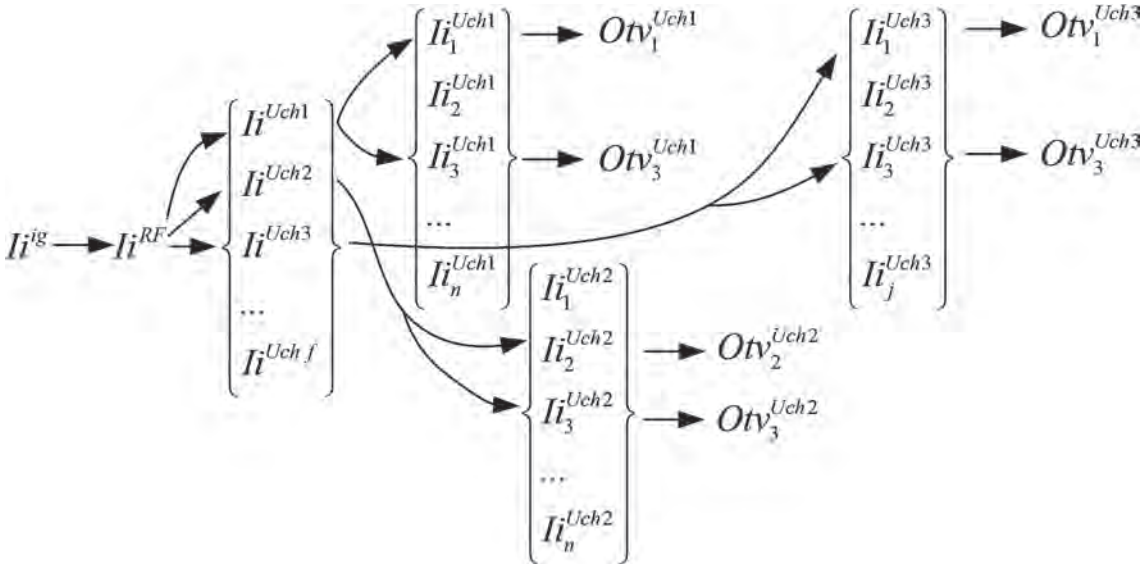

Рис. 6. Графическое отображение атаки из информационной инфраструктуры иностранного государства

где ali_{vid}^{Otv} – атакованная информационная инфраструктура, видимая ответственному лицу; ali_n – общее количество атакованной информационной инфраструктуры в рамках $attack$.

Применительно к нашему примеру (рисунок 6) информированность Otv_3^{Uch} в худшем случае будет 16%, а в лучшем (при условии, что он осведомлен о всех атаках на элементы информационной инфраструктуры участника СОИБ) – 33%.

Применение средств противодействия компьютерным атакам формализуется моделью, состоящей из процессов: регулирования настроек системы противодействия компьютерным атакам и средств администрирования безопасности информации, регулирования информационных и вычислительных ресурсов критически важной информационной системы, регулирования управляющей информации[13].

Таким образом, каждое из действий характеризуется временным промежутком, затрачиваемым на него. Каждый из ответственных лиц запускает цикл противодействия атаке основной характеристикой которого будет, временной промежуток, затрачиваемый на его исполнение. Множество ответственных лиц породит множество циклов противодействия, разрозненных по времени, целям и подчиненных интересам различных систем управления.

Учитывая, что циклы противодействия могут выполняться параллельно друг другу, то общее время, затраченное на противодействие атаке, будет определяться временем завершения последнего цикла. При этом не обязательно, что цикл, завершившийся последним, будет самым длительным во времени. В общем случае время, затраченное на общий цикл противодействия ($t_{общ}^{прот}$) определяется следующим образом:

$$t_{общ}^{прот} = \Delta t + t_{цикл}^{посл}$$

где Δt – период времени с момента обнаружения первой атаки, до момента начала работы цикла завершившегося последним; $t_{цикл}^{посл}$ – время длительности работы цикла завершившегося последним.

Обобщенная характеристика структур для действий в киберпространстве (на примере США)

Рассматривая противника (блок НАТО), в первую очередь необходимо рассмотреть США как головную структуру в области кибербезопасности и киберпространства (все остальные страны блока НАТО в подавляющем большинстве используют документы, созданные на базе руководящих документов США). Основными структурами для действий в киберпространстве является Агентство национальной безопасности (АНБ) в связке с Центральным разведывательным управлением (ЦРУ) и киберкомандование США.

АНБ осуществляет радиоэлектронную разведку и обеспечение информационной безопасности в интересах правительства США.

Радиоэлектронная разведка осуществляет сбор информации о планах, намерениях, возможностях и местонахождении террористических групп, организаций, иностранных держав, или их агентов, которые угрожают национальной безопасности США. В качестве примера систем шпионажа можно привести PRISM, обработкой больших данных занимаются множество дата-центров созданных в интересах АНБ и ЦРУ[14]. В рамках обеспечения ИБ осуществляется защита жизненно важных национальных систем США, коммуникационных сетей США и информации от кражи или нанесения ущерба противником, а также обеспечивается доступность и подлинность информации, необходимой правительственным структурам США. Обеспечение информационной безопасности и радиоэлектронной разведки необходимы для проведения разведывательных операций в киберпространстве киберкомандованием США и их партнерами.

В свою очередь киберкомандование США планирует, координирует, объединяет, синхронизирует и проводит мероприятия по руководству операциями и защите компьютерных сетей министерства обороны; готовит и осуществляет полный спектр военных операций в киберпространстве, обеспечивает свободу действий США и их союзников в киберпространстве и препятствует аналогичным действиям противника.

Таким образом, противник, осуществляя атаку, представляет из себя единую структуру – киберкомандование иностранного государства. Действует скоординированно по четкому плану, имеет высокую степень информированности, резерв сил и средств, которые может вводить их на различных этапах атаки, тем самым регулируя атакующие усилия по различным элементам.

С другой стороны, противнику противостоят разрозненные по силам, времени, планам, низкоинформированные (в рамках общей атаки противника) силы и средства, которые при этом рассосредоточены и подчинены различным системам управления.

В таблице приведены основные характеристики описываемой ситуации.

13 Климов С.М., Сычёв М. П., Астрахов А .В. «Противодействие компьютерным атакам. Методические основы». Электронное учебное издание [Электронный ресурс] URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-metod.htm

14 Как АНБ и ЦРУ используют дата-центры и облака [Электронный ресурс] URL: https://habr.com/ru/companies/vdsina/articles/531972/

Таблица 1.

Основные характеристики распределенной атаки со стороны противника и СОИБ

Противник	СОИБ
Атака планируется и осуществляется одной структурой – киберкомандованием.	Защита осуществляется различными структурами (являющимися участниками СОИБ), зачастую не связанными между собой.
Единая система управления.	Множество систем управления.
Единый план, четко разбитый на этапы по времени. Возможность корректировки плана по ходу операции.	У каждого участника свой собственный план противодействия, составленный исходя из его информированности и опыта. Циклы противодействия разобщены.
Высокая степень скоординированности и информированности в рамках проведения атаки.	Низкая степень скоординированности и информированности (между участниками СОИБ), ограниченная только собственными элементами.
Единая нормативная база.	Разный набор нормативных документов у участников.

Выводы

Информационная инфраструктура РФ является структурным элементом киберпространства и регулярно подвергается деструктивным воздействиям.

Очевидна несоизмеримость организованного множества воздействий, осуществляемых по единому замыслу и плану со стороны противника на информационную инфраструктуру и разрозненными, разноплановыми и взаимоисключающими мероприятиями по защите элементов информационной инфраструктуры, реализуемых не соподчинёнными должностными лицами.

Исход конфликта между множеством возможных источников деструктивных воздействий и объектов информационной инфраструктуры в большей степени будет зависеть не от средств защиты, а от скоординированности и информированности участников конфликтной ситуации, характеристик и порядка функционирования используемого фрагмента киберпространства.

Противник пытается доминировать в киберпространстве за счет технологического превосходства и повсеместного внедрения иностранного оборудования, протоколов и т.д.

Литература

1. *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.*
2. *Закалкин П. В. Эволюция систем управления киберпространством // Вопросы кибербезопасности. 2022. № 1(47). С. 76–86. DOI:10.21681/2311-3456-2022-1-76-86.*
3. *Белов А. С., Добрышин М. М., Шугуров Д. Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2022. № 11. С. 34–40.*
4. *Добрышин М. М. Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2022. № 2. С. 214–222.*
5. *Леонов Н. В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель. // Вопросы кибербезопасности. 2024. № 2(60). С.87–92. DOI: 10.21681/2311-3456-2024-2-87-92.*
6. *Левшун Д. С., Веснин Д. В., Котенко И. В. Прогнозирование категорий уязвимостей в конфигурациях устройств с помощью методов искусственного интелекта // Вопросы кибербезопасности. 2024. № 3(61). С.33–69 DOI: 10.21681/2311-3456-2024-3-33-39.*
7. *Иванов М. В., Калашников И. В., Нурулаев М. М. Исследование структурных свойств сети интернет на основе метаграфовых моделей // Труды СПИИРАН. 2020. Т.19. № 4. С. 880–900.*
8. *Мещеряков Р. В., Исхаков С. Ю. Исследование методов формирования индикаторов компрометации от внутренних источников информационных и киберфизических систем // Вопросы кибербезопасности. 2023. № 6(58) С.35–49. DOI:10.21681/2311-3456-2023-6-35-49.*
9. *Израилов К. Е., Буйневич М. В. Метод обнаружения атак различного генезиса на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3(55) С.90–100. DOI:10.21681/2311-3456-2023-3-90-100.*
10. *Иванов С. А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 86–90.*

References

1. *Starodubcev Ju. I., Zakalkin P. V., Ivanov S. A. Strukturno-funkcional'naja model' kiberprostranstva // Voprosy kiberbezopasnosti. 2021. № 4(44). S.16–24. DOI:10.21681/2311-3456-2021-4-16-24.*
2. *Zakalkin P. V. Jevoljucija sistem upravlenija kiberprostranstvom // Voprosy kiberbezopasnosti. 2022. № 1(47). S. 76–86. DOI:10.21681/2311-3456-2022-1-76-86.*
3. *Belov A. S., Dobryshin M. M., Shugurov D. E. Nauchno-metodicheskij podhod k ocenivaniju kachestva sistem obespechenija informacionnoj bezopasnosti // Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2022. № 11. S. 34–40.*
4. *Dobryshin M. M. Vybor struktury i mehanizmov adaptivnogo upravlenija sistemy obespechenija informacionnoj bezopasnosti // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2022. № 2. S. 214–222.*
5. *Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 1. Ontologicheskaja model'. // Voprosy kiberbezopasnosti. 2024. № 2(60). S.87–92. DOI: 10.21681/2311-3456-2024-2-87-92.*
6. *Levshun D. S., Vesenie D. V., Kotenko I. V. Prognozirovanie kategorij ujazvimostej v konfiguracijah ustrojstv s pomoshh'ju metodov iskusstvennogo intellekta // Voprosy kiberbezopasnosti. 2024. № 3(61). S.33–69 DOI: 10.21681/2311-3456-2024-3-33-39.*
7. *Ivanov M. V., Kalashnikov I. V., Nurullaev M. M. Issledovanie strukturnyh svojstv seti internet na osnove metagrafovyh modelej // Trudy SPIIRAN. 2020. T.19. № 4. S. 880–900.*
8. *Meshherjakov R. V., Ishakov S. Ju. Issledovanie metodov formirovanija indikatorov komprometacii ot vnutrennih istochnikov informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. 2023. № 6(58) S.35–49. DOI:10.21681/2311-3456-2023-6-35-49.*
9. *Izrailov K. E., Bujnevich M. V. Metod obnaruzhenija atak razlichnogo genezisa na slozhnye ob#ekty na osnove informacii sostojanija. Chast' 1. Predposylki i shema // Voprosy kiberbezopasnosti. 2023. № 3(55) S.90–100. DOI:10.21681/2311-3456-2023-3-90-100.*
10. *Ivanov S. A. Ustojchivost' setej svjazi obshhego pol'zovanija v uslovijah globalizacii // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2021. № 9. S. 86–90.*