13. *Borisov V.V., Kruglov V.V., Fedulov A.S.* Nechetkie modeli i seti [Fuzzy models and networks]. Moscow: Goryachaya liniya – Telekom, 2007.
14. *Herrera F., Lozano M.* Fuzzy Adaptive Genetic Algorithms: design, taxonomy, and future directions, *Soft Computing*. 7(2003). Springer-Verlag, 2003, pp. 545-562.
15. *Michael A., Takagi H.* Dynamic control of genetic algorithms using fuzzy logic techniques, *Proc. of the 5th International Conference on Genetic Algorithms*. Morgan Kaufmann, 1993, pp. 76-83.
16. *Lee M.A., Takagi H.* Integrating design stages of fuzzy systems using genetic algorithms, *Proceedings of the 2nd IEEE International Conference on Fuzzy System*, 1993, pp. 612-617.
17. *King R.T.F.A., Radha B., Rughooputh H.C.S.* A fuzzy logic controlled genetic algorithm for optimal electrical distribution network reconfiguration, *Proceedings of 2004 IEEE International Conference on Networking, Sensing and Control, Taipei, Taiwan, 2004*, pp. 577-582.
18. *Herrera F., Lozano M.* Adaptation of genetic algorithm parameters based on fuzzy logic controllers. In: F. Herrera, J.L. Verdegay (eds.) Genetic Algorithms and Soft Computing, Physica-Verlag, Heidelberg, 1996, pp. 95-124.
19. *Rutkovskaya D., Pilin'skiy M., Rutkvoskiy L.* Neyronnye seti, geneticheskie algoritmy i nechetkie sistemy [Neural networks, genetic algorithms and fuzzy systems]. Moscow: Goryachaya liniya – Telekom, 2006.
20. *Gladkov L.A., Gladkova N.V., Gusev N.Y., Semushina N.S.* Integrated approach to the solution of computer-aided design problems, *Proceedings of the 4th International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'19). Advances in Intelligent Systems and Computin*g. Vol. 875. Springer, Cham, 2020, pp. 246-257.

Статью рекомендовал к опубликованию д.т.н., профессор С.М. Ковалев.

Гладков Леонид Анатольевич – Южный федеральный университет; e-mail: lagladkov@sfedu.ru; г. Таганрог, Россия; тел.: 88634371625; кафедра САПР; к.т.н., доцент.

Гладкова Надежда Викторовна – e-mail: nvgladkova@sfedu.ru; тел.: 88634393260; кафедра САПР; старший преподаватель.

Ясир Муханад Джаббар – e-mail: yasir_82@mail.ru; тел.: 88634371625; кафедра САПР; аспирант.

Gladkov Leonid Anatol'evich – Southern Federal University; e-mail: lagladkov@sfedu.ru; Taganrog, Russia; phone: +78634371625; the department of CAD; cand. of eng. sc.; associate professor.

Gladkova Nadezhda Viktorovna – e-mail: nvgladkova@sfedu.ru; phone: +78634393260; the department of CAD; senior teacher.

Yasir Mukhanad Jabbar – e-mail: yasir_82@mail.ru; phone: +78634371625; the department of CAD; postgraduate student.

УДК 004.7 DOI 10.18522/2311-3103-2021-4-243-255

И.В. Родыгина, И.И. Бузенков, Ю.В. Каханец

КОНЦЕПЦИЯ ПОСТРОЕНИЯ И АРХИТЕКТУРА КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СЕГМЕНТОВ РЕГИОНАЛЬНОЙ ИНФОКОММУНИКАЦИОННОЙ СЕТИ

На сегодняшний день, в абсолютном измерении, ни одна отрасль государства не обходится без современных высокотехнологичных средств связи, соединяющих вычислительные системы и удалённые базы данных. Использование новых информационных и коммуникационных технологий в качестве средства разрешения противоречий, а также средства неявного воздействия, на мировой арене становится нарастающей угрозой для безопасности сообщества. В представленной работе рассматриваются не только этапы развития, но и основные тенденции, подходы к построению цифровых информационных систем, а также характерные

угрозы информационной безопасности для них. Также в статье показано актуальное место критически важных информационных сегментов в общем контексте системы связи Российской Федерации. В первой части работы раскрывается концепция трёхкомпонентного построения региональных критически важных информационных сегментов. В основной части акцент сделан на различии технологий, применяемых для построения критически важных информационных сегментов. Основная часть статьи нацелена на выявление уязвимостей сложных информационных структур и систем, в которых используются архитектуры мультисервисных систем связи. Проведённый авторами анализ позволяет классифицировать основные угрозы информационной безопасности как для систем связи, построенных по классическим схемам коммутации каналов, так и для систем связи основанных на новых технологических принципах, в основе своей – коммутации пакетов. В целом авторы говорят нам, что идея стандартной и чётко определённой структуры трафика и процедур взаимодействия пользователей независимо от их типа, географической удалённости или области её применения совместно с цифровыми методами передачи и коммутации оказывает революционную роль в развитии систем связи. Особого внимания заслуживает представленная авторами классификация протоколов, которая признакам позволяет выявить наиболее слабые места в современных информационных системах, на которые нужно обратить внимание в первую очередь: протоколы, обеспечивающие функционирование беспроводных сетей, почтовые протоколы, протоколы файлового обмена и другие.

Информационно-коммуникационная сеть; критически важный информационный сегмент; технология; мультисервисная сеть связи; телефония.

I.V. Rodygina, I.I. Buzenkov, Yu.V. Kakhanets

CONSTRUCTION CONCEPT AND ARCHITECTURE CRITICAL INFORMATION SEGMENTS OF THE REGIONAL INFOCOMMUNICATION NETWORK

Today, in absolute terms, not a single branch of the state can do without modern high-tech communications that connect computing systems and remote databases. The use of new information and communication technologies as a means of resolving contradictions, as well as a means of implicit influence, is becoming a growing threat to the security of the community on the world stage. The presented work examines not only the stages of development, but also the main trends, approaches to the construction of digital information systems, as well as the characteristic threats to information security for them. The article also shows the actual place of critical information segments in the general context of the communication system of the Russian Federation. The first part of the work reveals the concept of a three-component construction of regional critical information segments. The main part focuses on the difference in technologies used to build critical information segments. The main part of the article is aimed at identifying the vulnerabilities of complex information structures and systems that use the architecture of multiservice communication systems. The analysis carried out by the authors allows us to classify the main threats to information security both for communication systems built according to classical circuit switching schemes, and for communication systems based on new technological principles, basically - packet switching. In general, the authors tell us that the idea of a standard and clearly defined traffic structure and user interaction procedures, regardless of their type, geographic distance or area of its application, together with digital transmission and switching methods, has a revolutionary role in the development of communication systems. Special attention should be paid to the classification of protocols presented by the authors, which allows to identify the weakest points in modern information systems, which should be paid attention to first of all: protocols that ensure the functioning of wireless networks, mail protocols, file exchange protocols, and others.

Information and communication network; critical information segment; technology; multiservice communication network; telephony.

Введение. Развитие и стремительное объединение информационных технологий и систем связи ярко обострило актуальность вопросов информационной безопасности в них. Западными специалистами в области информационной безопасности в ходе оценки роли информационно-технических воздействий (далее –

ИТВ) на отдельно взятую информационную инфраструктуру был проведён анализ сопоставимости финансовых потерь при применении традиционных средств воздействия и принципиально новых форм (кибератаки). При этом западные эксперты считают кибератаки наиболее экономически выгодными, потому что 1 млн. долларов и двадцать человек, проводя компьютерные атаки, могут обеспечить успех, сопоставимый с действиями многотысячной группировки войск. 10 млн. долларов и пятьдесят человек могут дезорганизовать государственную и критически важную информационную инфраструктуру (КВИИ) противника более чем на неделю. 30 млн. долларов и сто человек способны вывести из строя экономическую информационную инфраструктуру таким образом (рис. 1), что на её восстановление уйдут годы [1, 2].

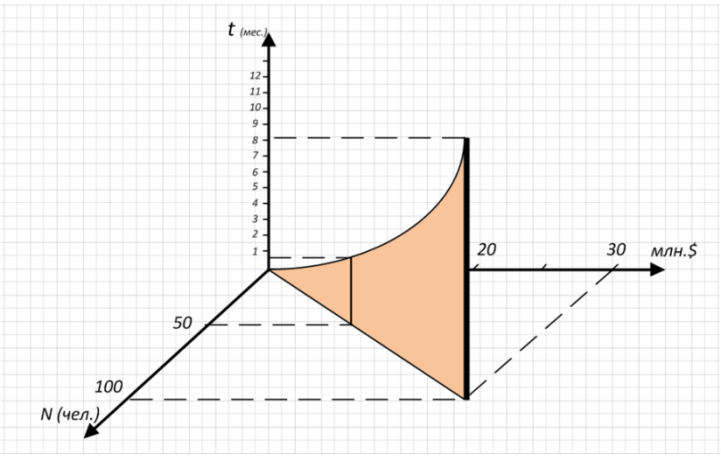

Рис. 1. Вероятность ущерба КВИИ от воздействия сил кибероперaций

Использование информационных и коммуникационных технологий (далее – ИКТ) в качестве средства разрешения противоречий, а также средства неявного воздействия на КВИИ государственного и экономического управления становится нарастающей угрозой как внутренней, так и международной безопасности.

Концепция трёхкомпонентного построения интегрированной инфокоммуникационной сети регионов (ИКС-Р). Мировое развитие информационных технологий, эволюция существующей системы связи Российской Федерации, ее техническое и технологическое состояние обусловили необходимость создания ИКС-Р, обеспечивающей автоматизацию управленческих функций, интеграцию специальных и информационных систем с целью обеспечения возможности комплексного использования информации баз данных и услуг связи должностными лицами органов муниципального и регионального управления на всех уровнях [2]. Основным функциональным предназначением ИКС-Р является обеспечение доступа к мультисервисным услугам связи конечным пользователям выделенного информационного сегмента региона [3]. Концепция трёхкомпонентного построения ИКС-Р приведена на рис. 2.

Связь Российской Федерации – одна из отраслей экономики РФ, а также обширная сфера деятельности по предоставлению услуг связи, осуществляющая сбор, хранение и передачу информации в рамках законодательства РФ. Сегодня ни одна отрасль государства не обходится без специалистов по информационным технологиям и связи. Техническую основу связи РФ представляют объединённые совокупности сетей, служб и оборудования связи, расположенных и функционирующих на

территории РФ. Эти совокупности, по функционалу и являются составными частями ИКС-Р, а по сути, критически важными информационными сегментами, которые предназначены для удовлетворения потребностей населения, органов государственной власти, административного управления, обороны, безопасности, охраны правопорядка, а также хозяйствующих субъектов региона в мультисервисных услугах связи [3, 4]. Анализ, проведённый доминирующими телекоммуникационными гигантами РФ (Вымпелком, Ростелеком, МТС), показал, что основной услугой, оказываемой ИТКС-Р в России является телефония (в том числе IP-телефония) – это почти 65% от всего объёма трафика.

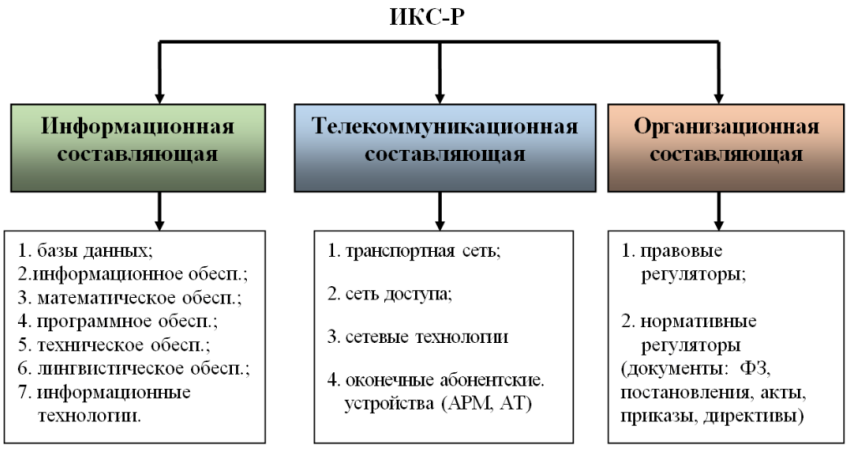

Рис. 2. Концепция построения региональной информационно-коммуникационной сети

Критически важный информационный сегмент (далее – сегмент) телефонной сети ИКС-Р – это комплекс технических сооружений и оборудования, предназначенный для осуществления телефонной связи и состоящий из телефонных узлов связи, телефонных станций, линий связи и абонентских терминалов [4]. Ключевыми узлами сегментов ИКС-Р являются автоматизированные телефонные станции (АТС) – технологический комплекс, предназначенный для коммутации каналов связи телефонной сети. На сегодняшний день АТС являются современными специализированными компьютерами с таблицами маршрутизации и серверным оборудованием, способные обслуживать до нескольких тысяч абонентов одновременно. Помимо высокого качества передачи речевого трафика, АТС предоставляют пользователям ряд специализированных абонентских услуг: от записи и переадресации вызова, до высокоскоростного доступа к ресурсам ГИС Internet.

Линии связи, которые соединяют телефонные сегменты могут быть кабельными, воздушными, радиорелейными, лазерными (оптоволоконными), спутниковыми, то есть, в сегментах используются все возможные физические линии связи первичной сети (рис. 3). В последние годы всё больше используются смешанные каналы (с преобладанием оптоволокна) функционирующие по принципам коммутации пакетов и облачных вычислений. Объединение линий связи первичной сети представляет собой транспортные сети. Транспортная сеть (связи) – сеть связи, обеспечивающая перенос (транспортирование) и распределение разнородного трафика между сетями доступа, в которые включены вызывающий и вызываемый пользователи [5]. На данный момент времени общепринятая классификация транспортных сетей представлена следующим образом:

Рис. 3. Роль сегментов телефонной связи в рамках системы связи РФ

1) Сеть (связи) транспортная магистральная – часть транспортной сети, обеспечивающая перенос разнородного трафика с заданным качеством между региональными сетями.

2) Сеть (связи) транспортная региональная – часть транспортной сети, обеспечивающая подключение сетей доступа для предоставления установленного набора услуг заданного качества пользователям.

3) Сеть (связи) местная – часть региональной сети, имеющая выход на сетевой узел региона, или автономная сеть, обеспечивающая предоставление услуг заданного качества компактно размещенным пользователям.

В настоящее время протокол IP (Internet Protocol – правило межсетевого взаимодействия) де-факто стал базовым протоколом транспортных сетей, а IP-(мультисервисные) сети используются в качестве транспортных. При этом протокол сетевого уровня IP, как и было задумано его разработчиками, используется в транспортных сетях для объединения разнородных сетей, построенных с использованием технологий, функционирующих на нижележащих уровнях модели OSI [6, 7]. Протокол IP – это основной протокол передачи пакетов в составных сетях, состоящих из большого количества разнородных (по технологиям) локальных сетей. Как средство объединения разнотипных сетей. Протокол IP организует пакетную передачу информации от узла к узлу IP-сети, не используя процедур установления соединения между источником и приемником информации. Он является дейтаграммным протоколом: при передаче информации по протоколу IP каждый пакет передается от узла к узлу и обрабатывается в узлах независимо от других пакетов. Для региональных телефонных сегментов ИКС-Р наравне с технологиями стеков TCP/IP широко используются все технологии первичных транспортных сетей связи [8]:

- технологии первичных сетей – синхронной цифровой иерархии (SDH), SDH следующего поколения (NG-SDH), технологии спектрального мультиплексирования, плезиохронной (PDH) цифровой иерархии;
- технологии волоконно-оптических систем передачи и спектрального мультиплексировния (xWDM);
- технологии оптических транспортных сетей (OTN);

♦ пакетных технологий – асинхронного режима переноса (ATM), FrameRelay, гигабит-Ethernet (GE, 10/40/100 GE), многопротокольной коммутации по меткам (технология MPLS) и другие.

Предоставление конечному пользователю услуг высококачественной и высокоскоростной мультисервисной связи обеспечивается доступ ко внешним сетям по правилам QoS:

1. Сети цифровой связи с интеграцией услуг (ISDN);
2. Сети IP-телефонии;
3. Пакетная передача данных и доступ к ресурсам ГИС Internet.

ISDN сети. ISDN (Integrated Services Digital Network) – это цифровая сеть с интеграцией услуг (рис. 4).

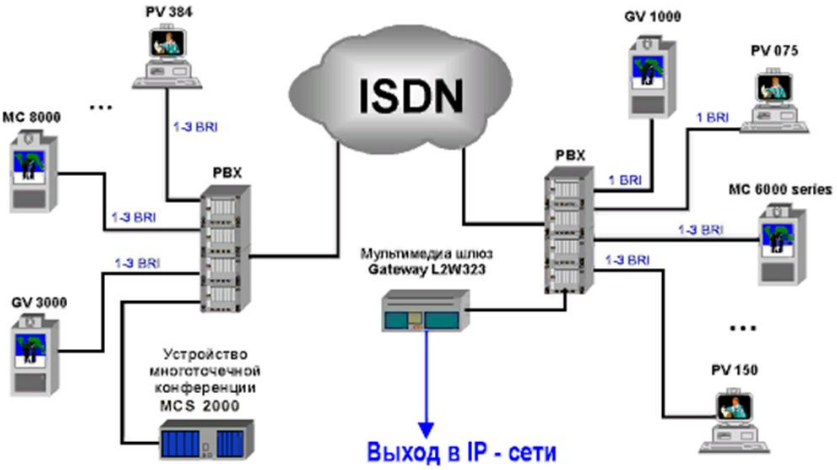

Рис. 4. Использование технологии ISDN в сегментах ИКС-Р

Услуги ISDN предоставляемые сетью интересны в основном корпоративным клиентам, следовательно, и использовать их будут организации, предприятия и специальные ведомства устанавливая необходимые платы на свои АТС СВА. По отношению к другим телекоммуникационным технологиям в телефонии ISDN считается относительно защищенной технологией. Но, тем не менее, при классическом подходе к защите информации проверки на отсутствие НДВ на оборудовании (платах и серверах ISDN) в стандартном списке сертификации, как правило, не проводятся [10].

Сервис IP-телефонии. Доступ абонентов сегмента ИКС-Р к услугам IP-телефонии производится за счет соответствующего оборудования, установленного в слотах станции в виде стандартных плат. Центральным компонентом IP-телефонии является сервер (шлюз), который отвечает за соединение телефонной и IP-сетей, т.е. он подключен к телефонной сети и может дозвониться до любого абонентского терминала (телефона) и получить доступ к сети передачи данных (например, ГИС Internet), то есть может получить доступ к любому компьютеру или IP-телефону (рис. 5). Обязательным элементом сети IP-телефонии является абонентский терминал (АТ), который может быть реализован как программным (например, Cisco IP SoftPhone), так и аппаратным способом (например, Cisco EP Phone, который подключается напрямую к Ethernet-порту коммутатора). Причем в первом случае звонки можно осуществлять даже через домашний компьютер, оснащенный звуковой картой и микрофоном, а во втором случае, в качестве або-

нентского пункта выступает АТ IP-телефон. Еще одним компонентом архитектуры IP-телефонии можно назвать специализированные пользовательские приложения, которые появились благодаря развитию компьютерных технологий интеграции голоса, видео и данных в единые потоки данных (Call-центры, системы унифицированной обработки сообщений) [11, 12]. В свою очередь, свободный доступ технологий IP-телефонии к трафику и ресурсам АТ создаёт своеобразный спектр проблем, связанных с обеспечением информационной безопасности абонента. Во всех современных сегментах ИКС-Р реализована система разграничения доступа абонентов к услугам связи или сервисам, предоставляемым сетью. В некоторых ЦАТС программное разделение может насчитывать до 1000 различных категорий абонентов. Выполняется это, системным администратором. Но на практике, для скорости обслуживания, более 100 категорий не разделяют в сети [13–15].

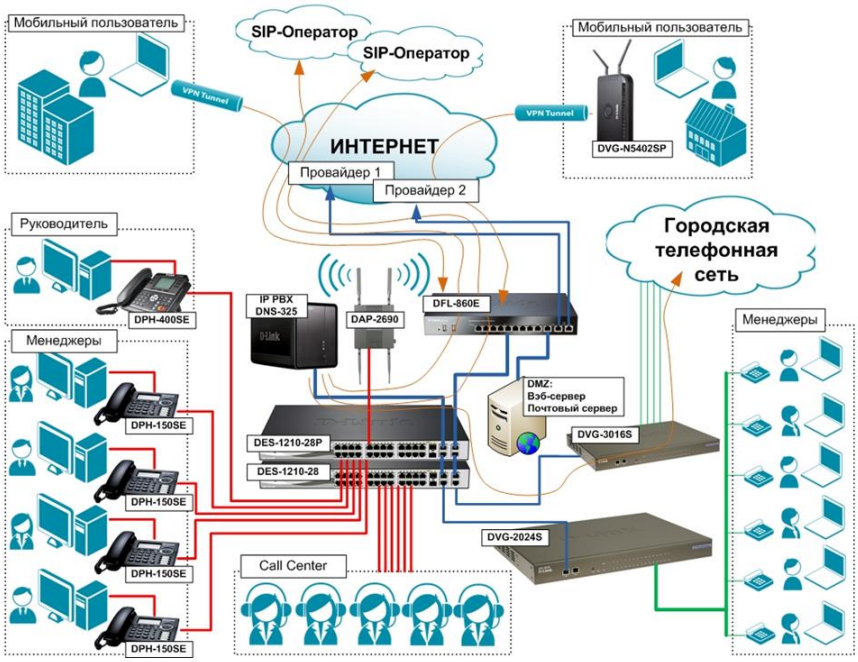

Рис. 5. Организация IP-телефонии в сегментах ИКС-Р

Так же существуют возможности организации абонентских групп и создания для них доступа к определенному списку функционала аппаратно-программных средств АТС (ФАПС). В современных системах эта организация реализована на программном уровне. Ограничивают данное разделение, в основном, физические параметры АТ групп абонентов. Так же реализация некоторых сервисов требует установления дополнительного оборудования на АТС сегмента [16]. Присвоение абоненту (выделенной группе абонентов) категорий определяется специальными матрицами, которые и определяют ФАПС для той или иной группе (абоненту). ФАПС характеризует перечень мультисервисных услуг связи. Этот перечень зависит от типа и возможностей оборудования, а также от настроек, осуществлённых администратором ЦАТС.

Классификация протоколов, используемых в ИКС-Р для осуществления информационных процессов. Кроме стека TCP/IP существует плеяда протоколов, которые так или иначе влияют на информационную безопасность КВИИ. Протоколы обмена информацией становятся основным цементирующим материалом для по-

строения распределённых систем обмена и обработки цифровой информации [17–19]. Такие протоколы особенно важны при рассмотрении общей архитектуры сети, то есть всей совокупности связей технических и программно-аппаратных элементов. Исходя из известного функционала уровней модели OSI возможно составить определённую классификацию протоколов и их функциональное определение. Именно идея стандартной и чётко определённой структуры обмениваемой информации и процедур взаимодействия пользователей независимо от их типа, географической удалённости или области применения совместно с цифровыми методами передачи и коммутации оказывает революционную роль в развитии ИКС-Р.

В табл. 1 приведена классификация наиболее распространённых на сегодняшний день протоколов с учётом их влияния на информационную безопасность. Данное разбиение протоколов по различным признакам позволяет выявить наиболее характерные «болезненные точки» и очаги уязвимостей [20], на которые нужно обратить внимание в первую очередь: протоколы, обеспечивающие функционирование беспроводных сетей, почтовые протоколы, протоколы файлового обмена и другие.

Заключение. Таким образом, проведённый анализ и представленная классификационная схема протоколов информационного обмена позволяет сформулировать перечень основных угроз для информационной безопасности сегмента ИКС-Р:

1) Возможность удалённого доступа практически к любому ресурсу и АТ сети (проблематика правил межсетевого взаимодействия и управления протоколами сети);

2) Потенциальная угроза доступа через backdoor's в аппаратной компоненте КВИИ (проблематика унификации технологического оборудования сети) [21];

3) Угроза, связанная с человеческим фактором (проблематика возможности несанкционированного доступа и эффект внутреннего нарушителя – «недобросовестный администратор»).

В дальнейшем, при планировании стратегии защиты информационных ресурсов сегмента ИКС-Р мы можем учитывать каждую из перечисленных моделей угроз и наиболее эффективно осуществлять организационные (работа с персоналом) и технические мероприятия по осуществлению информационной безопасности сети.

Таблица 1

Классификация протоколов, используемых в ИКС-Р для осуществления информационных процессов

№ п/п	Градация по классификационному признаку	Технология/ тип протокола	Уровень реализации модели OSI	Функционал	Обеспечение безопасности
1) По принадлежности к сетям ИКС-Р (среде передачи)					
1.1	Глобальных сетей	MPLS; TDM; FDM; TDMA; CDMA; WDMA; Ethernet; FDDI; PPP; Token Ring; Технологии и протоколы беспроводного доступа (п.6);	Все уровни ЭМВОС	Обеспечение доступа к ресурсам ИТКС; Информационный обмен	На уровнях ЭМВОС: Прикладной-сетевой
1.2	Региональных сетей	MPLS; TDM; FDM; TDMA; CDMA; WDMA; Ethernet; FDDI; PPP; Token Ring; Технологии и протоколы беспроводного доступа (п.6);	Все уровни ЭМВОС	Обеспечение доступа к ресурсам ИТКС; Информационный обмен	На уровнях ЭМВОС: Прикладной-сетевой
1.3	Локальных сетей	MPLS; TDM; FDM; TDMA; CDMA; WDMA; Ethernet; FDDI; PPP; Token Ring; Технологии и протоколы беспроводного доступа (п.6);	Все уровни ЭМВОС	Обеспечение доступа к ресурсам ИТКС; Информационный обмен	На уровнях ЭМВОС: Прикладной-сетевой
1.4	Наложенных сетей	MPLS; TDM; FDM; TDMA; CDMA; WDMA; Ethernet; FDDI; PPP; Token Ring; Технологии и протоколы беспроводного доступа (п.6);	Все уровни ЭМВОС	Обеспечение доступа к ресурсам ИТКС; Информационный обмен	На уровнях ЭМВОС: Прикладной-сетевой

№ п/п	Градация по классификационному признаку	Технология/ тип протокола	Уровень реализации модели OSI	Функционал	Обеспечение безопасности
1.5	Прикладных сетей	MPLS; TDM; FDM; TDMA; CDMA; WDMA; Ethernet; FDDI; PPP; Token Ring; Технологии и протоколы беспроводного доступа (п.6);	Все уровни ЭМВОС	Обеспечение доступа к ресурсам ИТКС; Прикладной информационный обмен ИТКС (АСУ, СЭД)	На уровнях ЭМВОС: Прикладной-сетевой
1.6	Беспроводных сетей	3G, 4G, NFC, IrDA, Bluetooth, 802.15.4 (16,17)	Физический	Обеспечение доступа к ресурсам ИТКС (передача данных, VoIP, туннелирование, многопротокольная маршрутизация, мультиплексирование, адресация	Не обеспечивается
		802.11	Канальный		Не обеспечивается
1.7	Доступа к среде передачи	USB; HDMI; X.25; FR; IEEE-1394; Технологии и протоколы беспроводного доступа (п.6); TCP; UDP; RUDP; TALI; ITOT; RDP; RPC; DNS; MPLS; TDM; FDM; TDMA; CDMA; WDMA; Ethernet; FDDI; PPP; Token Ring; GRE; L2F; L2TP; ATMP; PPTP; RAS; H.245; H.225	Сеансовый; Транспортный; Сетевой; Канальный; Физический	Обеспечение доступа к ресурсам ИТКС (передача данных, VoIP, туннелирование, многопротокольная маршрутизация, мультиплексирование, адресация, файловый обмен, управление	На уровнях ЭМВОС: сеансовый - сетевой
2) По уровням ЭМВОС					
2.1	Прикладного уровня	DCAP; SNTP; DHCP; Finger; FTP; HTTP; S-HTTP; IMAP; POP3; IMAP4; IRCP; LDAP; MIME; BOOTP; IPDC; ISAKMP; NTP; SNMP; Radius; RLOGIN; RTCP; SMTP; TELNET; TACACS+; X-Window	Прикладной	Почтовые, управления, файлового обмена, безопасности	S-HTTP; S- MIME; TACACS+; Radius; ISAKMP; IPSec
2.2	Представительского уровня	LPP, SSL, TLS	Представления	Обеспечение безопасности	SSL, TLS
2.3	Сеансового уровня	DNS, NetBIOS/IP, PAP, RTCP, RPC, L2TP, L2F, SOCKS, PPTP	Сеансовый	Управления, VoIP, обеспечение безопасности, туннелирование	SOCKS, PPTP, PAP, L2TP, L2F
2.4	Транспортного уровня	TCP, UDP, RUDP, TALI, ITOT, RDP	Транспортный	Управление, файловый обмен, адресация	Не обеспечивается
2.5	Сетевого уровня	BGP, EGP, IPv4(6), ICMP, ARP, IRDP, RARP, NHRP, OSPF, RIP, VRRP, IGMP, MARS, IPSec	Сетевой	Маршрутизация, безопасность, управление, файловый обмен, адресация	IPSec
2.6	Канального уровня	ARP, PPP, FDDI, Ethernet, VLAN, PPTP, Token Ring	Канальный	Многопротокольная маршрутизация, безопасность, мультиплексирование, VoIP, туннелирование, адресация	PPTP
2.7	Физического уровня	USB; HDMI; X.25; FR; IEEE-1394; Технологии и протоколы беспроводного доступа (п.6)	Физический	Обеспечение доступа к высшим уровням ЭМВОС, физическая среда распространения инф.	Физическая защита доступа к ресурсам ИТКС

№ п/п	Градация по классификационному признаку	Технология/ тип протокола	Уровень реализации модели OSI	Функционал	Обеспечение безопасности
3) По назначению					
3.1	Управления	SNMP, NTP, DHCP, Whois, RLOGIN, TELNET, ICMP, BOOTP, WCCP, TCP, SMTP	Прикладной, сетевой, канальный, представления	Управление протокольного сопровождения процесса обмена данными	Не обеспечивается
3.2	Обеспечения безопасности	SSH, S-HTTP, S-MIME, ESP, Oakley, AH, ISAKMP/IKE, SSL, TLS, IPSec, PPTP, L2TP, L2F, MPPE, MSCHAP, WEP, Kerberos, PAP, TACACS, CHAP, Radius	Прикладной, сетевой, канальный, транспортный	Обеспечение безопасности процесса обмена данными	Обеспечивается
3.3	Почтовые	IMAP, POP3, IMAP4, SMTP, MIME	Прикладной	Обеспечение процесса обмена сообщениями почтовых служб	Не обеспечивается
3.4	Файлового обмена	FTP, TFTP, LDAP, TCP, TELNET, IP, UDP, RUDP	Прикладной, сетевой, канальный, транспортный	Обеспечение процесса файлового обмена	Не обеспечивается
3.5	Маршрутизации	BGMP, IGMP, MARS, MDGP, MSDP, MZAP, PGM, OSPF, RIP, VRRP, IGRP, EGP	Сетевой	Обеспечение процесса маршрутизации по правилам стека протоколов TCP/IP	Не обеспечивается
3.6	Многопротокольной маршрутизации	MPLS-IGP, MPLS-TE, GMPLS	Канальный	Обеспечение процесса маршрутизации по правилам стека протоколов TCP/IP	Не обеспечивается
3.7	Мультиплексирования	MPLS, TDM, FDM, CDMA, WDMA, Ethernet, FDDI, PPP, Token Ring	Канальный	Обеспечение процесса мультиплексирования инкапсулированных данных	Не обеспечивается
3.8	Передачи данных	PDH, SDH, ATM, X.25, IEEE-1394, FR, USB, RS, GRID, P2P, WDMA	Канальный; Физический	Обеспечение процесса передачи данных	Не обеспечивается
3.9	Беспроводных сетей	3G, 4G, NFC, IrDA, Bluetooth, 802.15.4 (16,17)	Физический, канальный	Обеспечение процесса функционирования беспроводных сетей	Не обеспечивается
3.10	Туннелирования	GRE, L2F, L2TP, ATMP, PPTP	Сеансовый, канальный	Обеспечение процесса туннелирования	Не обеспечивается
3.11	VoIP	RAS, H.225, H.245	Сеансовый, канальный	Обеспечение процесса оцифровки речевой информации (голос-по-IP)	Не обеспечивается
3.12	Реального времени	CAN, NTP	Прикладной	Обеспечение временных синхронизмов	Не обеспечивается

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Саенко И.Б., Лаута О.С., Карпов М.А.* Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. – 2021. – № 1. – С. 41.
2. *Дементьев В.Е.* Угрозы инфотелекоммуникационной сети в условиях информационного противоборства. – СПб., 2015. – 16 с.
3. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ.
4. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ. Москва, 2006. Москва, 2017.
5. *Редькин Ю.В., Бузенков И.И., Чернышева Е.М.* Анализ конфигураций беспроводных сетей систем сбора данных и управления // Информационные технологии. Радиоэлектроника. Телекоммуникации. – 2020. – № 8. – С. 357.
6. *Берзин Е.А.* Оптимальное распределение ресурсов и элементы синтеза систем. – М.: Советское радио, 1974. – 303 с.

7. *Рахманов А.А.* Сетецентрические системы управления: закономерные тенденции, проблемные вопросы и пути их решения // Военная мысль. – 2010. – № 10. – С. 41-50.
8. *Бузенков И.И., Редькин Ю.В., Чернышев В.М.* Применение аппаратно-программного комплекса в системах сбора и обработки телеметрической информации // Компьютерные технологии в инженерной и исследовательской деятельности: Матер. Всероссийской научно-технической конференции с международным участием. Таганрогский государственный радиотехнический университет. – 2000. – С. 301-306.
9. *Полковникова Н.А., Бузенков И.И.* Разработка гибридных экспертных систем и интеллектуальных систем поддержки принятия решений. – Новороссийск, 2018.
10. *Редькин Ю.В., Бузенков И.И., Чернышева Е.М.* Организация морской сети передачи данных с применением mesh-технологии // Информационные ресурсы и системы в экономике, науке и образовании: Сб. статей X Международной научно-практической конференции / под ред. А.П. Ремонтова. – Пенза, 2020. – С. 100-105.
11. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
12. *Радько Н.М., Скобелев И.О.* Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М.: РадиоСофт, 2011. – 229 с.
13. *Коцыняк М.А., Карпов М.А., Лаута О.С., Дементьев В.Е.* Управление системой обеспечения безопасности информационно-телекоммуникационной сетью на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. – 2020. – № 4. – С. 3-10.
14. *Саати Т.* Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 278 с.
15. *Савин Л.В.* Сетецентричная и сетевая война. Введение в концепцию. – М.: Евразийское движение, 2011. – 130 с.
16. *Седякин Н.М.* Элементы теории случайных импульсных потоков. – М.: Советское радио, 1965. – 264 с.
17. *Лаута О.С., Нечепуренко А.П., Муртазин И.Р., Суетин А.И.* Модели интеллектуальных воздействий // Сб. «Информационная безопасность регионов России». – 2017. – С. 144-145.
18. *Гудков М.А., Гагарин Ю.А., Крибель А.М., Соловьёв Д.В.* Применение методов захвата и анализа пакетов, передаваемых по информационно-телекоммуникационным сетям, для аудита сетевой безопасности сетей // Современные информационные технологии. Теория и практика: Матер. IV Всероссийской научно-практической конференции. Отв. ред. Т.О. Петрова. – 2018. – С. 158-162.
19. *Бесков А.В., Лаута О.С., Мамай А.В.* Архитектура сети подвижной радиосвязи на основе эталонной модели взаимодействия открытых систем // Радиолокация, навигация, связь: Сб. трудов XXV Международной научно-технической конференции в 6-ти т. Воронежский государственный университет, АО "Концерн "Созвездие". – 2019. – С. 173-182.
20. *Муртазин И.Р., Коцыняк М.А., Лаута О.С.* Функциональная модель комплекса информационного воздействия на беспроводные сети передачи данных // Актуальные проблемы защиты и безопасности: Тр. XXII Всероссийской научно-практической конференции РАРАН. – 2019. – С. 188-189.
21. *Коцыняк М.А., Карпов М.А.* Методика синтеза системы защиты информационно-телекоммуникационной сети // Радиолокация, навигация, связь: Сб. трудов XXVI Международной научно-технической конференции: в 6 т. Воронеж, 2020. – С. 231-236.
22. *Иванов Д.А., Карпов М.А., Коцыняк М.А., Шимаров Е.В.* Модель воздействия сетевых атак на беспроводные сети передачи данных специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: Сб. научных статей. Санкт-Петербург, 2020. – С. 166-171.

REFERNCES

1. *Saenko I.B., Lauta O.S., Karpov M.A.* Model' ugroz resursam ITKS kak klyuchevomu aktivu kriticheski vazhnogo ob"ekta infrastruktury [Model of threats to ITCS resources as a key asset of a critically important infrastructure object], *Elektrosvyaz'* [Telecommunication], 2021, No. 1, pp. 41.
2. *Dement'ev V.E.* Ugrozy infotelekommunikatsionnoy seti v usloviyakh informatsionnogo protivoborstva [Threats to the infotelecommunication network in the context of information warfare]. Saint Petersburg, 2015, 16 p.

3. Federal'nyy zakon "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii" ot 26.07.2017 N 187-FZ [Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated 26.07.2017 N 187-FZ].
4. Federal'nyy zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" ot 27.07.2006 N 149-FZ. Moskva, 2006. Moskva, 2017 [Federal Law "On Information, Information Technologies and Information Protection" dated 27.07.2006 N 149-FZ. Moscow, 2006. Moscow, 2017].
5. *Red'kin Yu.V., Buzenkov I.I., Chernysheva E.M.* Analiz konfiguratsiy besprovodnykh setey sistem sbora dannykh i upravleniya [Analysis of configurations of wireless networks of data collection and management systems], *Informatsionnye tekhnologii. Radioelektronika. Telekommunikatsii* [Information technologies. Radio electronics. Telecommunications], 2020, No. 8, pp. 357.
6. *Berzin E.A.* Optimal'noe raspredelenie resursov i elementy sinteza system [Optimal resource allocation and elements of system synthesis]. Moscow: Sovetskoe radio, 1974, 303 p.
7. *Rakhmanov A.A.* Setetsentricheskie sistemy upravleniya: zakonomernye tendentsii, problemnye voprosy i puti ikh resheniya [Network-centric management systems: natural trends, problematic issues and ways to solve them], *Voennaya mysl'* [Military thought], 2010, No. 10, pp. 41-50.
8. *Buzenkov I.I., Red'kin Yu.V., Chernyshev V.M.* Primenenie apparatno-programmnogo kompleksa v sistemakh sbora i obrabotki telemetricheskoy informatsii [Application of hardware and software complex in systems for collecting and processing telemetric information], *Komp'yuternye tekhnologii v inzhenernoy i issledovatel'skoy deyatel'nosti: Mater. Vserossiyskoy nauchno-tekhnicheskoy konferentsii s mezhdunarodnym uchastiem. Taganrogskiy gosudarstvennyy radiotekhnicheskiy universitet* [Computer technologies in engineering and research activities: Materials of the All-Russian Scientific and Technical Conference with international participation. Taganrog State Radio Engineering University], 2000, pp. 301-306.
9. *Polkovnikova N.A., Buzenkov I.I.* Razrabotka gibridnykh ekspertnykh sistem i intellektual'nykh sistem podderzhki prinyatiya resheniy [Development of hybrid expert systems and intelligent decision support systems]. Novorossiysk, 2018.
10. *Red'kin Yu.V., Buzenkov I.I., Chernysheva E.M.* Organizatsiya morskoy seti peredachi dannykh s primeneniem mesh-tekhnologii [Organization of a marine data transmission network using mesh technology], *Informatsionnye resursy i sistemy v ekonomike, nauke i obrazovanii: Sb. statey X Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Information resources and systems in economics, science and education: Collection of articles of the X International Scientific and Practical Conference], ed. by A.P. Remontova. Penza, 2020, pp. 100-105.
11. GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniya [GOST R 50922-2006. Information protection. Basic terms and definitions].
12. *Rad'ko N.M., Skobelev I.O.* Risk-modeli informatsionno-telekommunikatsionnykh sistem pri realizatsii ugroz udalennogo i neposredstvennogo dostupa [Risk models of information and telecommunication systems in the implementation of threats of remote and direct access]. Moscow: RadioSoft, 2011, 229 p.
13. *Kotsynyak M.A., Karpov M.A., Lauta O.S., Dement'ev V.E.* Upravlenie sistemoy obespecheniya bezopasnosti informatsionno-telekommunikatsionnoy set'yu na osnove algoritmov funktsionirovaniya iskusstvennoy neyronnoy seti [Management of the information and telecommunication network security system based on artificial neural network functioning algorithms], *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki* [Proceedings of Tula State University. Technical sciences], 2020, No. 4, pp. 3-10.
14. *Saati T.* Prinyatie resheniy. Metod analiza ierarkhiy [Decision-making. Method of hierarchy analysis]. M.: Radio i svyaz', 1993, 278 p.
15. *Savin L.V.* Setetsentrichnaya i setevaya voyna. Vvedenie v kontseptsiyu [Network-centric and network warfare. Introduction to the concept]. Moscow: Evraziyskoe dvizhenie, 2011, 130 p.
16. *Sedyakin N.M.* Elementy teorii sluchaynykh impul'snykh potokov [Elements of the theory of random pulse flows]. Moscow: Sovetskoe radio, 1965, 264 p.
17. *Lauta O.S., Nechepurenko A.P., Murtazin I.R., Suetin A.I.* Modeli intellektual'nykh vozdeystviy [Models of intellectual impacts], *Sb. «Informatsionnaya bezopasnost' regionov Rossii»* [Collection "Information security of Russian regions"], 2017, pp. 144-145.

18. *Gudkov M.A., Gagarin Yu.A., Kribel' A.M., Solov'ev D.V.* Primenenie metodov zakhvata i analiza paketov, peredavaemykh po informatsionno-telekommunikatsionnym setyam, dlya audita setevoy bezopasnosti setey [Application of methods for capturing and analyzing packets transmitted over information and telecommunication networks for auditing network security of networks], *Sovremennye informatsionnye tekhnologii. Teoriya i praktika: Mater. IV Vserossiyskoy nauchno-prakticheskoy konferentsii* [Modern information technologies. Theory and practice: Materials of the IV All-Russian Scientific and Practical Conference]. ed. by T.O. Petrova, 2018, pp. 158-162.
19. *Beskov A.V., Lauta O.S., Mamay A.V.* Arkhitektura seti podvizhnoy radiosvyazi na osnove etalonnoy modeli vzaimodeystviya otkrytykh sistem [Architecture of a mobile radio communication network based on a reference model of interaction of open systems], *Radiolokatsiya, navigatsiya, svyaz': Sb. trudov XXV Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii v 6-ti t. Voronezhskiy gosudarstvennyy universitet, AO "Kontsern "Sozvezdie"* [Radar, navigation, communication: Proceedings of the XXV International Scientific and Technical Conference in 6 volumes. Voronezh State University, JSC Concern Constellation], 2019, pp. 173-182.
20. *Murtazin I.R., Kotsynyak M.A., Lauta O.S.* Funktsional'naya model' kompleksa informatsionnogo vozdeystviya na besprovodnye seti peredachi dannykh [Functional model of the complex of information impact on wireless data transmission networks], *Aktual'nye problemy zashchity i bezopasnosti: Tr. XXII Vserossiyskoy nauchno-prakticheskoy konferentsii RARAN* [Actual problems of protection and security: Proceedings of the XXII All-Russian Scientific and Practical Conference RARAN], 2019, pp. 188-189.
21. *Kotsynyak M.A., Karpov M.A.* Metodika sinteza sistemy zashchity informatsionno-telekommunikatsionnoy seti [Methodology of synthesis of the information and telecommunication network protection system], *Radiolokatsiya, navigatsiya, svyaz': Sb. trudov XXVI Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii: v 6 t. Voronezh, 2020* [Proceedings of the XXVI International Scientific and Technical Conference: in 6 vols. Voronezh, 2020], pp. 231-236.
22. *Ivanov D.A., Karpov M.A., Kotsynyak M.A., Shimarov E.V.* Model' vozdeystviya setevykh atak na besprovodnye seti peredachi dannykh spetsial'nogo naznacheniya [A model of the impact of network attacks on special-purpose wireless data transmission networks], *Aktual'nye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2020). IX Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya: Sb. nauchnykh statey* [fotelecommunications in science and education (APINO 2020). IX International Scientific-technical and scientific-methodical Conference: Collection of scientific articles]. Saint Petersburg, 2020, pp. 166-171.

Статью рекомендовал к опубликованию к.т.н. А.А. Полупанов.

Родыгина Ирина Владимировна – Государственный морской университет им. адмирала Ф.Ф. Ушакова; e-mail: habarova@mail.ru; г. Новороссийск, Россия; тел.: +79282284417; кафедра радиоэлектроники и информационных технологий; к.т.н.; доцент.

Бузенков Игорь Иванович – e-mail: igor.buzenkov@mail.ru; тел.: +79181567788; кафедра радиоэлектроники и информационных технологий; начальник кафедры; к.т.н.

Каханец Юлия Владимировна – e-mail: 266gr@mail.ru; тел.: +79184627956; магистрант.

Rodygina Irina Vladimirovna – Admiral Ushakov Maritime State University; e-mail: habarova@gmail.ru, Novorossiysk, Russia; phone: +79282284417; the department of radioelectronics and information technologies; cand. of eng. sc.; associate professor.

Buzenkov Igor Ivanovich – e-mail: igor.buzenkov@mail.ru; phone: +79181567788; the department of radioelectronics and information technologies; head of the department; cand. of eng. sc.

Kakhanets Yulia Vladimirovna – e-mail: 266gr@mail.ru; phone: +79184627956; master's student.