***ЭКОНОМИКА И КАЧЕСТВО СИСТЕМ СВЯЗИ*** ***№ 1(23) / 2022***

***ISSN 2500-1833***

*Международный научно-практический электронный журнал*
*Основан в 2015 году, издается ежеквартально*

***Учредители:***
*Региональное отделение Российской академии естественных наук,*
*АО «Национальный институт радио и инфокоммуникационных технологий»*

***Издатель:***
*АО «Национальный институт радио и инфокоммуникационных технологий»*



*Журнал публикует статьи, отражающие результаты исследований в соответствии со следующими разделами ГРНТИ:*
*06.00.00 – Экономика и экономические науки*
*10.00.00 – Государство и право. Юридические науки*
*14.00.00 – Народное образование. Педагогика*
*19.00.00 – Массовая коммуникация. Журналистика. СМИ*
*20.00.00 – Информатика*
*47.00.00 – Электроника. Радиотехника*
*49.00.00 – Связь*
*73.00.00 – Транспорт*
*82.00.00 – Организация и управление*
*84.00.00 – Стандартизация*
*90.00.00 – Метрология*

***Адрес редакции:*** *111024, Москва, ул. Авиамоторная, дом 8А, стр. 5.*
*АО «НИРИТ»*
***Тел./факс:*** *8 (495)133-38-99 (282)* ***e-mail:*** *ekss@nirit.org* ***сайт:*** *http://nirit.org/*

# СОДЕРЖАНИЕ

## ЭКОНОМИКА И УПРАВЛЕНИЕ



## СЕТИ И СИСТЕМЫ СВЯЗИ



## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



## ПЕДАГОГИКА

# ЭКОНОМИКА И УПРАВЛЕНИЕ

## РОЛЬ СИСТЕМЫ СВЯЗИ В ВЫПОЛНЕНИИ ОСНОВНЫХ ЗАДАЧ МЧС РОССИИ

***В.В. Макаров,*** *д.э.н., профессор, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, akad.makarov@mail.ru;*
***Т.А. Блатова,*** *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, nsnlon@gmail.com.*

***УДК 654.1.***

***Аннотация.*** Основные задачи Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий требуют максимальной оперативности их выполнения и минимального времени для принятия управленческих решений. Качественное управление в чрезвычайных ситуациях невозможно без надежных сетей и современных средств связи.

***Ключевые слова:*** система связи; чрезвычайные ситуации; МЧС; надежность; информационная безопасность.

## THE ROLE OF THE TELECOMMUNICATION SYSTEM IN FULFILLING THE MAIN TASKS OF THE MINISTRY OF EMERGENCY SITUATIONS OF RUSSIA

***Vladimir Makarov****, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
***Tatyana Blatova****, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

***Annotation.*** The main tasks of the Ministry of Emergency Situations require maximum efficiency of their implementation and minimum time for making managerial decisions. High-quality management in emergency situations is impossible without reliable networks and modern means of telecommunication.

***Keywords:*** telecommunication system; emergencies; the Ministry of Emergency Situations; reliability; information security.

### Введение

Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС России) решает широкий круг задач в области безопасности жизнедеятельности населения и участвует в обеспечении национальной безопасности. Реализация этих задач позволяет улучшить не только показатели благополучия граждан, но и показатели социально-экономического развития государства. Обеспечение минимальных рисков для людей и социальной инфраструктуры способствуют притоку инвестиций, которые обеспечивают рост экономики и социальной сферы.

Надежная организация обмена необходимой информацией с заданными показателями качества обслуживания является залогом успешного решения основных задач МЧС России. Основу информационного обмена составляет

информационно-телекоммуникационная инфраструктура, надежность которой является ключевым фактором эффективного функционирования цифровой экономики [1]. При сборе, обработке и обмене информацией обязательным условием является соблюдение требований информационной безопасности в соответствии с российским законодательством.

**Требования к системе связи МЧС России при выполнении конкретных задач**

В соответствии с Положением о МЧС России основными задачами МЧС России являются:

- выработка и реализация государственной политики в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности, а также безопасности людей на водных объектах в пределах компетенции МЧС России;
- организация подготовки и утверждения в установленном порядке проектов нормативных правовых актов в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах;
- осуществление управления в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности, безопасности людей на водных объектах, а также управление деятельностью федеральных органов исполнительной власти в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций;
- осуществление нормативного регулирования в целях предупреждения, прогнозирования и смягчения последствий чрезвычайных ситуаций и пожаров, а также осуществление специальных, разрешительных, надзорных и контрольных функций по вопросам, отнесенным к компетенции МЧС России;
- осуществление деятельности по организации и ведению гражданской обороны, экстренному реагированию при чрезвычайных ситуациях, защите населения и территорий от чрезвычайных ситуаций и пожаров, обеспечению безопасности людей на водных объектах, а также осуществление мер по чрезвычайному гуманитарному реагированию, в том числе за пределами Российской Федерации [2].

Требования органов государственного управления зависят от особенностей субъекта Федерации и его муниципальных образований, но существует ряд общих положений, которые следует считать универсальными. Эти положения можно сформулировать в виде перечня функциональных задач, решаемых при помощи системы связи МЧС России:

- оперативное предоставление всем должностным лицам, список которых утвержден заранее, информации о возникших нештатных ситуациях или потенциальных угрозах;
- поддержка работы Системы-112 для организации эффективной работы экстренных оперативных служб;
- бесперебойное функционирование общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (ОКСИОН) как составной части Российской единой системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС),

предназначенной для защиты населения и территорий от чрезвычайных ситуаций природного, техногенного и иного характера;
- взаимодействие Центра управления в кризисных ситуациях (ЦУКС) с ситуационными центрами, созданными органами государственного управления и предприятиями повышенной опасности, с возможностью проведения сеансов видео-конференц-связи и обмена другой информацией;
- отображение актуальной информации на специально установленных уличных экранах, а также в средствах массовой информации, используя, в частности, возможности «бегущей строки».

Решение перечисленных задач ставит ряд сложных требований организационного и технического характера. В состав требований субъектов экономики, в зависимости от характера их деятельности, могут входить все положения, перечисленные выше. С практической точки зрения дополнительно следует выделить пять важных аспектов:
- обеспечение работы систем мониторинга (различного назначения) для выявления нештатных ситуаций и прогнозирования потенциальных угроз;
- передача предварительно записанных сообщений ограниченной группе абонентов за счет установления коммутируемого соединения через телефонную сеть общего пользования;
- отображение актуальной информации на мониторах персональных компьютеров, включенных в локальную вычислительную сеть предприятия;
- рассылка сообщений *SMS* на мобильные телефоны сотрудников и абонентов, находящихся на территории предприятия;
- возможность поддержки нового направления в обеспечении комплексной безопасности, основанного на широком использовании различного рода телеметрических устройств, функционирующих в автоматическом режиме.

При наличии специфических требований субъектов экономики их руководители должны заранее договориться с территориальными органами МЧС России о методах решения задач, которые могут возникать в силу технологических, географических, демографических и иных факторов.

К требованиям социального характера относятся положения, определяемые особенностями реакции населения на критические ситуации. Отдельно учитываются требования людей с ограниченными возможностями. К таким положениям, в дополнение к перечисленным выше, следует отнести:
- рассылку сообщений *SMS* на мобильные телефоны всех абонентов, находящихся в зоне, которую (по решению специалистов МЧС России или иных ведомств) необходимо покинуть;
- обращение (через телефоны фиксированной и мобильной связи, а также терминалы, подключенные к сети интернет) к волонтерам с просьбой оказать помощь лицам с ограниченными возможностями;
- прием сигналов о помощи с терминалов типа «социальная розетка», если они установлены в квартирах или иных жилых помещениях.

Развитие подсистемы радиосвязи МЧС России определяется следующими основными факторами:
- усложнением задач, решаемых подразделениями МЧС России и изменением их организационно-штатной структуры;

- опережающим развитием инфокоммуникационных технологий в областях цифровой обработки сигналов и протоколов связи;
- техническим заделом в области средств и систем радиосвязи, имеющимся на предприятиях промышленности России.

К негативным факторам, которые необходимо учитывать при планировании развития подсистемы радиосвязи МЧС России, необходимо отнести следующие:

- недостаточное финансирование разработок и закупок современных цифровых радиосредств и комплексов автоматизации управления техническими средствами узлов связи;
- отсутствие разветвленной инфраструктуры государственных и коммерческих операторов связи в ряде районов РФ;
- отставание в развитии отечественной элементной базы радиоэлектронных средств;
- разунификация средств радиосвязи, использующихся в МЧС России;
- разунификация средств радиосвязи взаимодействующих министерств и ведомств;
- ограниченный выделенный радиочастотный ресурс, особенно в КВ диапазоне.

Важнейшими факторами для успешной локализации и ликвидации возникшей чрезвычайной ситуации (ЧС) являются: время и оперативность, возможность принятия правильных решений и управление процессом ликвидации ЧС.

Для эффективного управления процессами локализации и ликвидации ЧС необходимо своевременно передавать с места и на место события разнообразную информацию, вести видеорепортаж или проводить видеоконференцию, обеспечивать телефонную связь и доступ к различным базам данных. Решение данных задач напрямую зависит от возможностей и характеристик используемой системы связи, которая образует каналы связи (КС) между органами управления (ОУ) и управляемыми объектами (УО), выполняет коммуникативную и транспортную функции и должна обладать свойствами универсальности, мобильности и оперативности при организации связи в различных условиях. При этом система связи МЧС России построена по иерархическому принципу в соответствии со структурой Министерства.

Системе связи свойственны конечные значения показателей надежности и качества обслуживания трафика, влияющие на эффективность информационного обмена между ОУ и УО. Наличие в системе связи резервных каналов и оборудования, возможность организации обходных путей или использования альтернативного оборудования и технологий позволяют снизить воздействие помех на КС и (или) их отказов на функционирование системы в целом и обеспечить своевременное и качественное решение поставленных задач.

Особую роль в структуре системы связи МЧС России играет мобильная составляющая, образуемая системами спутниковой и радиосвязи, к преимуществам которой относится:

- высокая живучесть при ликвидации чрезвычайных ситуаций;
- оперативность установления связи на различные расстояния;
- возможность организации связи в движении и через труднодоступные пространства.

Таким образом, ролью системы связи в системе управления МЧС России является надежная организация обмена необходимой информацией с заданными показателями качества обслуживания. Требования к системе связи МЧС России должны рассматриваться применительно к каждой из конкретных задач, решаемых системой связи МЧС России.

***Требования по устойчивости, непрерывности и оперативности управления***

Под устойчивостью функционирования понимается способность системы связи МЧС выполнять свои функции при выходе из строя части элементов в результате воздействия дестабилизирующих факторов. С точки зрения основного критерия последствий воздействия внешних дестабилизирующих факторов в тексте ГОСТ Р 53111-2008 выделяется доля элементов системы связи, вышедших из строя. Используются три градации ущерба: высокий, средний и низкий, для которых максимальная доля неработоспособных элементов составляет 50%, 30% и 10% соответственно [3].

Под непрерывностью функционирования понимается свойство системы связи МЧС предоставлять основные услуги с перерывами во времени, которые не превышают заранее установленные нормы. Основными считаются те виды услуг, которые напрямую связаны с оперативной работой всех подразделений МЧС России.

Под оперативностью управления понимается способность системы связи МЧС изменять свою топологию и алгоритмы предоставления услуг для обеспечения максимальной эффективности решения возникающих задач. Оперативность управления зависит от требований в части функций контроля системы связи МЧС, а также от квалификации обсуживающего персонала.

Устойчивость и непрерывность функционирования системы связи МЧС России, а также оперативность управления ее ресурсами должна обеспечиваться за счет реализации следующих положений:

- проектирование и построение с использованием отказоустойчивых топологий на уровне транспортной (первичной) сети;
- применение отечественных аппаратно-программных средств как для создания, так и для дальнейшего развития системы связи МЧС;
- оснащение всех устанавливаемых аппаратно-программных средств постоянно обновляемой системой информационной безопасности;
- организация процессов технической эксплуатации, предусматривающих оперативное устранение отказов;
- привлечение к решению возникающих задач по управлению высококвалифицированных специалистов;
- использование ресурсов других операторов связи для поддержки нормированных качественных показателей;
- проведение периодических проверок базовых свойств устойчивости и непрерывности системы связи МЧС, а также оперативности функций управления ее ресурсами.

***Требования по надежности***

Под надежностью (*dependability*), согласно ГОСТ Р 27.102-2021, понимается свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность объекта выполнять требуемые функции в заданных режимах, условиях применения, стратегиях технического

обслуживания, хранения и транспортирования. Надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его применения может включать в себя безотказность, долговечность, ремонтопригодность и сохраняемость или определенные сочетания этих свойств [4].

Готовность (*availability*) – это способность объекта выполнять требуемые функции в заданных условиях, в заданный момент или период времени при условии, что все необходимые внешние ресурсы обеспечены.

Безотказность (*reliability*) определяет свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки в заданных режимах и условиях применения.

Ремонтопригодность (*maintainability*) – это свойство объекта, заключающееся в его приспособленности к поддержанию и восстановлению работоспособности объекта путем технического обслуживания и ремонта.

Из приведенных определений в соответствии с [4] и сложностью задач, решаемых системой связи МЧС России, следует необходимость учета множества факторов, которые влияют на показатели надежности.

Один из важнейших показателей надежности – коэффициент готовности *(availability factor)*. Он равен вероятности того, что в данный момент времени объект находится в работоспособном состоянии, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается [4].

Обеспечение норм, соответствующих современным международным требованиям, достигается за счет реализации комплекса мер. Из них наиболее важным следует считать:

- выбор структуры, основанной на отказоустойчивых топологиях;
- применение оборудования передачи, коммутации и обработки информации, отвечающего всем требованиям, а также прошедшего необходимый объем испытаний;
- установка и постоянное обновление комплексной системы информационной безопасности;
- организация эффективной системы технической эксплуатации, способной оперативно решать возникающие задачи;
- заключение с операторами связи, у которых арендуются ресурсы любого вида, соглашения об уровне обслуживания (*SLA*).

Пять положений, перечисленных выше, должны учитываться при детальной разработке концепции построения и развития системы связи МЧС на этапе составления технического задания на оборудование для реализации предлагаемых научно обоснованных решений, а также при проектировании, строительстве и эксплуатации.

***Требования по помехоустойчивости***

Под помехоустойчивостью для автоматизированной системы любого рода понимается ее способность выполнять свои функции в условиях воздействия помех, в частности – от электромагнитных полей. Применительно к системе связи МЧС помехоустойчивость следует рассматривать и как результат влияний естественных факторов, присущих всем видам телекоммуникационного оборудования, так и как последствия воздействий преднамеренного характера.

Обеспечение требуемой помехоустойчивости достигается за счет реализации комплекса организационно-технических мероприятий, разработка которого представляет предмет самостоятельного исследования. Для численной

оценки помехоустойчивости системы связи МЧС в целом следует использовать показатель допустимой вероятности искажения информации.

***Требования по мобильности***

Термин «мобильность» в международной практике используется для обозначения двух видов связи. Мобильный, как перевод слова «*mobile*», указывает на возможность связи при перемещении терминала в широких географических пределах. Например, интернет стал по-настоящему «мобильным», что подтверждают данные, приведенные в [5]. В перспективе мобильность будет обеспечена при нахождении терминала в любой точке Земного шара и его тропосфере при перемещении с высокой скоростью. Мобильный, как перевод прилагательного «*nomadic*», указывает на перемещение терминала с невысокой скоростью и, как правило, в пределах ограниченной территории.

В первом случае функции мобильности поддерживаются сетями, основанными на сотовой топологии (вне зависимости от используемого стандарта). Во втором случае, обычно применяются так называемые системы профессиональной мобильной радиосвязи (ПМР), работающие в диапазоне ультракоротких волн (УКВ). Сети ПМР обычно создаются на базе звездообразной и древовидной топологий.

Сети ПМР выполняют важные функции в системе связи МЧС. Их дальнейшее развитие предусматривает повышение качества связи, расширение перечня поддерживаемых услуг и снижение расхода энергии в терминальном оборудовании. Важнейший аспект эволюции ПМР – переход к обслуживанию мультимедийного трафика.

***Требования по пропускной способности, доступности и управляемости***

Термин «пропускная способность» используется как способность системы связи обслуживать трафик различной природы. В англоязычной технической литературе принято различать пропускную способность (*capacity*) и производительность (*throughput*). Пропускная способность определяет характеристики сети связи в части переноса информации (бит/с, кбит/с, Мбит/с, Гбит/с и Тбит/с). Производительность определяет характеристики в части функций коммутации и распределения информации. Для систем с коммутацией каналов единицей измерения служит количество соединений, устанавливаемых в единицу времени (чаще всего – за один час в период обработки максимального объема трафика). Для систем с коммутацией пакетов в качестве единицы измерения используется количество *IP*-пакетов, обрабатываемых за одну секунду.

Пропускная способность и производительность компонентов сети связи рассчитываются методами теории телетрафика на основании оценки объемов передаваемой и принимаемой информации с учетом заданных качественных показателей.

Под доступностью (*accessibility*) в рекомендации МСЭ-*T E.*800 понимается возможность получения услуги с нормированными характеристиками тогда, когда она нужна пользователю [6]. Для определения доступности следует учитывать совместный эффект, обусловленный временем распространения сигналов, процессами обслуживания трафика и характеристиками надежности телекоммуникационной системы и ее компонентов.

Термин «управляемость» (*controllability*) в теории телекоммуникационных сетей связан с возможностью перевести систему из одного состояния в другое. Для системы связи МЧС управляемость следует рассматривать с точки зрения того

объекта, к которому применяются соответствующие процедуры. Во-первых, объектом управления служат все системы связи, ресурсы которых задействованы в поддержке услуг, востребованных в интересах МЧС России. Во-вторых, объектом управления может быть только система связи МЧС. Возникающие организационные и технические проблемы уместно классифицировать как задачи верхнего и нижнего уровней соответственно.

В первом случае необходимо решать нетривиальные организационные и технические задачи, требующие, как правило, проведения большого объема исследований и согласований. Во втором случае возникают только технические задачи, но их сложность может заметно возрастать, если не решены задачи верхнего уровня.

***Требования по безопасности, своевременности и целостности информации***

В системе связи МЧС безопасность (*safety*) следует рассматривать, по крайней мере, с двух точек зрения. Во-первых, важную роль играют функции безопасности с точки зрения сохранения работоспособности системы связи МЧС как инструмента поддержки технологических процессов, входящих в сферу компетенции министерства. Во-вторых, существенное значение придается информационной безопасности с целью защиты данных от несанкционированного доступа.

Информационная безопасность должна обеспечиваться за счет применения современных аппаратно-программных средств. При этом программное обеспечение (ПО) должно регулярно обновляться с учетом частоты появления новых угроз информационной безопасности. Статистические данные свидетельствуют, что основным источником нарушения информационной безопасности остается так называемый «человеческий фактор». Для снижения соответствующего риска должны быть разработаны и доведены до сведения персонала, использующего средства связи, регламенты обмена информацией, ее обработки, хранения и распространения.

Своевременность (*timeliness*) также уместно рассматривать с двух точек зрения. Во-первых, этот термин относится к вероятностно-временным показателям процесса доставки информации. Во-вторых, он используется для нормирования процесса развертывания мобильных комплексов связи, предназначенных для работы на той территории, где возникла ЧС или иная нештатная ситуация. Обеспечение своевременности доставки информации достигается корректным проектированием сети связи и выполнением всех работ, предусмотренных регламентами технического обслуживания, включая процедуры управления ресурсами при чрезмерном росте трафика.

Термин «целостность» (*integrity*) применительно к информации имеет несколько толкований. В рекомендации МСЭ-*T F.*400/*X.*400 определяются «целостность содержимого» и «целостность последовательности сообщений» [7]. Целостность содержимого дает возможность получателю убедиться в том, что исходное содержимое сообщения не было изменено. Целостность последовательности сообщений позволяет отправителю выдавать получателю подтверждение сохранности последовательности сообщений.

В рекомендации МСЭ-*T G.*701 определяется целостность последовательности битов. Под ней понимаются свойства цифрового канала связи или их совокупности, образующей тракт обмена информацией, передавать сигнал без каких-либо изменений [8]. В рекомендации МСЭ-*T I.*233.2 вводится понятие

целостности информации. Оно трактуется как состояние сети связи, при котором все кадры (фреймы) доставляются без ошибок за счет корректной проверки при помощи процедуры *FCS* (*Frame Check Sequence*) [9]. Эта процедура предусматривает формирование контрольной последовательности, необходимой для обнаружения ошибок передачи. В рекомендации МСЭ-*T M.*60 предложен термин «целостность услуги». Он определен как свойство сети по сохранению атрибутов уже предоставленной услуги в течение сеанса связи без ощутимого ухудшения для всех пользователей [10].

Для системы связи МЧС определение целостности информации, приведенное в рекомендации МСЭ-*T F.*400/*X.*400, представляется доминирующим. Следует подчеркнуть, что с точки зрения семиуровневой модели взаимодействия открытых систем обеспечение целостности информации зависит не только от характеристик сети связи. Важную роль играют функциональные возможности информационной системы, которая использует для доставки информации. Это означает, что целостность определяется свойствами сети связи и информационной системы МЧС.

***Показатели качества обслуживания трафика***

Для нормирования показателей качества обслуживания мультисервисного трафика следует использовать принципы, принятые теми международными организациями, которые занимаются стандартами в области связи и информатики. Они предусматривают нормирование пяти основных качественных показателей:

- среднее значение времени доставки сообщений;
- время, в течение которого будут доставлены 95% всех сообщений;
- допустимая вероятность потери сообщений;
- допустимая вероятность искажения передаваемой информации;
- минимальный коэффициент готовности тракта доставки сообщений.

При необходимости могут быть заданы дополнительные нормы на вероятностно-временные характеристики, касающиеся процесса доставки сигналов управления и оповещения. Введение дополнительных норм должно учитывать функциональные возможности системы связи МЧС. Процесс организации контроля показателей качества обслуживания трафика представляет собой технологически более сложную задачу [11].

На уровне *IP*-пакетов показатели качества обслуживания мультисервисного трафика для связи между двумя интерфейсами определены в рекомендации МСЭ-*T Y.*1541 [12]. Они заданы для четырех величин: *IPTD*, *IPDV*, *IPLR* и *IPER.* Эти показатели представлены в табл. 1.

Таблица 1.

| Класс *QoS* | *IPTD*, мс | *IPDV*, мс | *IPLR* | *IPER* |
|---|---|---|---|---|
| 0 | 100 | 50 | $10^{-3}$ | $10^{-4}$ |
| 1 | 400 | 50 | $10^{-3}$ | $10^{-4}$ |
| 2 | 100 | *Не нормируется* | $10^{-3}$ | $10^{-4}$ |
| 3 | 400 | | $10^{-3}$ | $10^{-4}$ |
| 4 | 1000 | | $10^{-3}$ | $10^{-4}$ |
| 5 | *Не нормируется* | | | |

| Класс *QoS* | *IPTD*, мс | *IPDV*, мс | *IPLR* | *IPER* |
|---|---|---|---|---|
| 6 | 100 | 50 | $10^{-5}$ | $10^{-6}$ |
| 7 | 400 | 50 | $10^{-5}$ | $10^{-6}$ |

Величина *IPTD* (*IP packet transfer delay*) определяет среднее значение задержки *IP*-пакетов между интерфейсами. Параметр *IPDV* (*IP packet delay variation*) представляет собой вариацию (джиттер) задержки *IP*-пакетов. Вероятность *IPLR* (*IP packet loss ratio*) нормирует долю потерянных *IP*-пакетов, которая допускается в сети. Значение *IPER* (*IP packet error ratio*) равно доле искаженных *IP*-пакетов, которые теряются. Это означает, что величина *IPER* – один из составляющих компонентов нормы *IPLR*.

Кроме показателей, приведенных выше, должны учитываться нормы, приведенные в рекомендациях МСЭ-*T* серий *P*, *Q* и *Y*.

**Заключение**

Система связи играет важное значение для осуществления управления в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности, безопасности людей на водных объектах, а также управления деятельностью федеральных органов исполнительной власти в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, а также осуществления мер по чрезвычайному гуманитарному реагированию, в том числе за пределами Российской Федерации.

Таким образом, ролью сети связи в системе управления МЧС России является надежная организация обмена необходимой информацией с заданными показателями качества обслуживания. В связи с вышесказанным, технико-экономическое обоснование стратегических подходов организации связи в системе МЧС России должно базироваться на принципах оценки экономического ущерба.

**Литература**

1. Makarov V.V., Blatova T.A., Fedorov A.V., Budagov A.S. Metrology In Ensuring The Quality Of Products And Services In Digital Economy // European Proceedings of Social and Behavioural Sciences EpSBS, Krasnoyarsk, 20-22 мая 2020 года / Krasnoyarsk Science and Technology City Hall. – Krasnoyarsk: European Proceedings, 2020. – P. 490-498.
2. Указ Президента Российской Федерации «Вопросы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий» от 11.07. 2004 № 868 // Собрание законодательства Российской Федерации. 2004. – № 28. Ст. 2882 с изм. и допол. в ред. от 30.12.2021.
3. «ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки» от 18.12.2008 // Официальное издание. – М.: Стандартинформ, 2019.
4. «ГОСТ Р 27.102-2021 Надежность в технике. Надежность объекта. Термины и определения» от 08.10.2021 // Официальное издание. – М.: ФГБУ «РСТ», 2021.
5. Макаров В.В., Старкова Т.Н., Устриков Н.К. Цифровая экономика: эволюция, со стояние и резервы развития // Журнал правовых и экономических исследований, 2019. – № 4. – С. 222-229.

6. Рекомендации МСЭ-Т Е.800 (09/2008) Определение терминов, относящихся к качеству обслуживания.
7. Рекомендации МСЭ-Т F.400/X.400 (06/1999) Обзор систем и служб обработки сообщений.
8. Рекомендации МСЭ-Т G.701 (03/1993) Словарь терминов цифровой передачи и мультиплексирования и импульсно-кодовой модуляции (РСМ).
9. Рекомендации МСЭ-Т I.233.2 (10/1991) Услуги передачи кадров в ISDN.
10. Рекомендации МСЭ-Т M.60 (03/1993) Термины и определения, относящиеся к техническому обслуживанию.
11. Макаров В.В., Протасов С.Н., Стародубов Д.О. Использование совокупности методов контроля для объективной оценки качества услуг мобильной связи // Проблемы современной экономики, 2017. – № 2 (62). – С. 202-204.
12. Рекомендация МСЭ-Т Y.1540 (2/2006) Требования к сетевым показателям качества для служб, основанных на протоколе IP.

## СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МАРКЕТИНГА В РЕСПУБЛИКЕ БЕЛАРУСЬ

***И.Н. Колесная***, *аспирант кафедры экономики, магистр экономических наук, Белорусский государственный университет информатики и радиоэлектроники, koliesnaia@mail.ru;*
***В.А. Давидович****, директор ООО «МГТ», аспирант кафедры банковской экономики Белорусский государственный университет, mgtp@tut.by;*
***В.В. Тышлек,*** *магистр бизнес-администрирования, директор ООО «Белспецкомплект», исследователь в области экономических наук, tyshlek@mail.ru.*

***УДК 658.8***

***Аннотация.*** Актуальность статьи обусловлена изменением экономической ситуации в Республике Беларусь, широким применением цифровых технологий в экономике, а также активным внедрением на белорусский рынок новых товаров и современных технологий их продвижения. Развитие маркетинга и продвижение собственных брендов становится основной задачей для белорусских предприятий в современной экономической ситуации.

***Ключевые слова:*** маркетинг; Республика Беларусь; современные тенденции; продвижение; реклама.

## MODERN TRENDS IN THE DEVELOPMENT OF MARKETING IN THE REPUBLIC OF BELARUS

***Irina Kolesnaya,*** *postgraduate student of the Department of Economics, Master of Economic Sciences, Belarusian State University of Informatics and Radioelectronics;*
***Vladimir Davidovich,*** *Director of MGT LLC, Belarusian State University; postgraduate student of the Department of Banking Economics;*
***Vitaly Tyshlek,*** *Master of Business Administration; LLC «Belspetskomplekt» director, researcher in the field of economic sciences.*

***Annotation.*** The relevance of the article is due to the change in the economic situation in the Republic of Belarus, the widespread use of digital technologies in the economy, as well as the active intrusion into the Belarusian market of new products and modern technologies for their promotion. The development of marketing and promotion of own brands is becoming the main task for Belarusian enterprises in the current economic situation.

***Keywords:*** marketing; Republic of Belarus; current trends; promotion; advertising.

**Введение**

Современная экономическая ситуация в Республике Беларусь характеризуется высокой степенью глобализации и информатизации бизнеса, ужесточением и изменением характера конкуренции на рынке. Для своего существования предприятие должно обеспечивать себе определенный уровень доходов. Оно может существовать только в том случае, если будет идти в ногу со временем и прогрессом. Исходя из этого, оно должно обеспечивать аккумулирование средств, позволяющих содержать себя, осуществлять обновление и усовершенствование своего производственного аппарата, и соответственно вести расширенное воспроизводство. Такое аккумулирование средств предприятие может обеспечить только при успешной реализации своего продукта на рынке.

**Проблемы и концепция развития маркетинга в Республике Беларусь**

Однако современный рынок весьма изменчив, а длительное игнорирование специфики товарного производства и роли рынка в Республике Беларусь привело к тому, что нынешнее поколение хозяйственных руководителей в большинстве своем не владеет необходимой теоретической базой и имеет слабый практический опыт работы на принципах экономической самостоятельности компаний. Поверхностное знакомство с методами комплектования портфеля заказов, налаживания производства, товародвижения и сбыта продукции, ориентированной на запросы потребителя, приводило и приводит к продвижению на рынок уже выпущенных товаров, не ставя перед собой задач исследования нужд и потребностей населения. Современная рыночная экономика Республики Беларусь не позволяет довериться воле рынка и отстраниться от потребностей населения. Чтобы сознательно влиять на ход продаж своего продукта, а тем самым получать доходы, необходимо занять по отношению к рынку активную позицию. Маркетинг и есть олицетворение такой позиции, нацеленной на создание того, что мы можем продать, а не сбыть то, что мы изготовили.

Многофункциональность рыночной деятельности, понимание особенностей в каждом конкретном случае и на каждом конкретном предприятии создало много различных подходов к устойчивому управлению предприятием в нестабильной рыночной среде. На основе личного опыта руководители, каждый по-своему, адаптируют деятельность своего предприятия и его систему управления к рыночным условиям. Однако, на сегодняшний день, большинство предприятий не определилось со стратегией своего поведения на рынке, их деятельность активна только на оперативном уровне. Это заметно, например, на рынке материалов, характеризующихся сезонностью спроса. Отсутствие стратегических концепций приводит к распылению сил и средств, к снижению эффективности управления материальными и финансовыми ресурсами и их потоками.

В условиях стремительного развития бизнеса в целом в Белоруссии, маркетинг набирает все больших оборотов. Причиной является конкуренция в

каждой отрасли хозяйства. Кроме того, в современных экономических условиях существенно возросла социально-экономическая роль маркетинга. Он стал нацеливать организации на более глубокое изучение потребностей населения. Здесь потребитель превращается в центральную фигуру, интересам которого подчиняется все производство. Для маркетинга, таким образом, главным становится то, что потребитель думает о своей покупке, в чем видит ее ценность, какие преимущества получает, приобретая тот или иной товар. Усилия организаций направляются на выявление знаний о товаре и понимание потребителей, на способности и умение маркетологов технически воплотить специфические потребности в реальный продукт, соответствующий вкусам и запросам потребителей. Реализация подобных функций маркетинга означает не только подчиненность сферы производства сфере потребления, но и окончательное превращение маркетинга в необходимый элемент хозяйственного механизма, обеспечивающего сочетание интересов производителя и потребителя как основы роста эффективного производства. Гарантом быстрых сроков окупаемости, высоких темпов эффективности продаж стала прогностическая функция маркетинга, направленная на точное определение приоритетных новых, еще неудовлетворенных потребностей, на их соизмерение и расчеты потенциальной эффективности их удовлетворения.

Таким образом, основным направлением маркетинга является определение ориентиров организации на настоящие и будущие нужды покупателей с созданием приемлемого предложения для удовлетворения существующих потребностей и получения прибыли.

Активный маркетинг на предприятии – это залог успеха. Проводя правильную маркетинговую политику, можно добиться очень успешных результатов. Не зря говорят в народе: «Продать можно, что угодно. Главное – знать как».

Поэтому, если не предоставлять маркетингу значимости, то можно потерять потребителя. Все дело в том, что маркетинг – это и реклама, и связь с покупателем, и изучение рынка, и способы донесения товара к потребителю и многое другое. Это большой комплекс мер, используя которые можно значительно повысить доход предприятия.

Современная концепция маркетинга состоит в том, что вся деятельность предприятия, включая капиталовложения, собственное производство, проведение и реализацию научно-технических исследований, использование рабочей силы, сбыт, сервисное обслуживание потребителей, должна быть основана на точном, заранее выверенном знании потребностей рынка. Концепция строится на учете всех условий производства и сбыта, как в ближайшей, так и в перспективе. Маркетинг является важной составной частью всего процесса управления производством. Его целью является обеспечение прибыли при минимальном коммерческом риске, а механизмом, обеспечивающим достижение этой цели – комплекс мероприятий по максимальному приспособлению всей деятельности предприятия и выпускаемых товаров к требованиям конкретных покупателей, выраженным через их платежеспособный спрос. Литературные источники нас информируют о том, что существует более 2000 определений маркетинга. По определению Ф. Котлера, «маркетинг – это вид человеческой деятельности, направленный на удовлетворение нужд и потребностей посредством обмена». И. Акулич, раскрывая данное определение, говорит, что «маркетинг как вид деятельности, прежде всего, предполагает:

- полное выявление нужд и потребностей покупателей;

- разработку и изготовление такого продукта, который необходим потребителю, с соответствующей упаковкой и обслуживанием;
- установление цен, приемлемых для потребителя и обеспечивающих достаточную прибыль производителю;
- доставку произведенных товаров в необходимом количестве в приемлемое для покупателя время и место;
- продвижение товара, включая рекламу, личную продажу, стимулирование продаж, создание благоприятного впечатления о товаре, фирме;
- управление маркетинговой деятельностью».

Субъекты хозяйствования в Республике Беларусь еще только осознают необходимость создания маркетинговой службы. Большинство малых и средних предприятий не имеют эффективных маркетинговых подразделений. Как правило, представители малого бизнеса не могут содержать маркетинговую службу. Кроме того, созданные службы зачастую занимаются только сбытом, в то время как в функции маркетинга входят исследования рынка, реализация проектов по продвижению товаров, разработка различных других программ, за которыми стоит большая аналитическая работа. Маркетинговая деятельность представляет собой комплекс мероприятий, ставящих целью исследование таких вопросов, как:

- изучение потребителя;
- исследование мотивов его поведения на рынке;
- анализ собственно рынка предприятия;
- исследование продукта (изделия или вида услуг);
- анализ форм и каналов сбыта;
- анализ объема товарооборота предприятия;
- изучение конкурентов, определение форм и уровня конкуренции;
- исследование рекламной деятельности;
- определение наиболее эффективных способов продвижения товаров на рынке;
- изучение «ниши» рынка.

Для реализации данного комплекса мероприятий зачастую необходимо значительное число работником, времени и средств.

Таким образом, маркетинг – это комплексная система организации производства и сбыта продукции, ориентированная на удовлетворение потребностей конкретных потребителей и получение прибыли на основе исследования и прогнозирования рынка, изучения внутренней и внешней среды предприятия, разработки стратегии и тактики поведения на рынке с помощью маркетинговых программ. Организация маркетинговой деятельности зависит от многих факторов: размера предприятия, видов и объемов производимой продукции, методов ее сбыта и технического обслуживания, специфики рынков сбыта и групп покупателей, условий конкуренции. Методологической основой оценки эффективности маркетинга является системный подход к деятельности предприятия на рынке, направленной на удовлетворение потребностей покупателей, создания при этом условий обеспечения рентабельности всей производственно-хозяйственной деятельности предприятия.

Современный этап развития маркетинга в Республике Беларусь предполагает высокий уровень стремления к совершенствованию и достижению более высокой эффективности. Организации стараются не отставать от западных

конкурентов, стараются использовать их опыт с некоторой подстройкой под специфические реалии хозяйственной деятельности.

Традиционный маркетинг всегда применялся с целью создания потребительских предпочтений и стимулирования спроса. Маркетинг будущего исходит из того, что мобильные устройства (смартфоны, планшеты и даже часы) становятся центром маркетинга. Стремительная эволюция девайсов и свободный доступ к интернету из любого места являются главными факторами влияния на формирование маркетинговых тенденций будущего. Мобильный маркетинг побуждает потенциальных клиентов совершать транзакции. В развитых странах в рамках мероприятий по оптимизации бизнеса сегодня широко применяется мобильная аналитика: производится обработка большого количества данных, поступающих через мобильные каналы, а затем осуществляется передача этих данных в более крупные автоматизированные информационные системы. Благодаря возможности охвата практически любой группы потребителей в режиме реального времени и оперативной передаче данных, мобильный маркетинг имеет все шансы стать главным инструментом управления взаимоотношениями с клиентами. Белорусский рынок пока не достиг достаточного уровня зрелости для полноценного функционирования мобильного маркетинга в рамках стратегий продвижения товаров и значительно отстает по применяемым технологиям от западных стран, в которых мобильный трафик уже давно обошел компьютерный. Это заставило многие компании по-другому взглянуть на продвижение бренда в сети. Сегодня интернет-магазины уже не только имеют мобильную версию своего сайта, но и предлагают приложения для смартфонов, чтобы пользователи могли быстро совершать покупки. Около 50% брендов активно ведут свои сообщества в социальных сетях, более 60% держат связь с клиентами через микроблоги. Более половины компаний (53%) платят за рекламу в соцмедиа, а 25% используют рекламу в приложениях. Среди трендов интернет-маркетинга на данный момент наблюдается тенденция повышения функциональности социальных сетей – 60% пользователей онлайн-ресурсов узнают новости именно из социальных сетей. Повышая внутреннюю функциональность, сети стремятся сосредоточить внимание пользователя на себе.

Например, в «Вконтакте» уже давно можно не только пообщаться с друзьями и поделиться фотографиями. Сеть предоставляет широкий спектр функций: бесплатное прослушивание музыки, просмотр фильмов, последние новости, обновления любимых компаний, игры и все это без перехода на другие сайты. Это предоставляет новые возможности маркетологам вовлекать аудиторию в свой бренд, используя персональные страницы или группы.

К тому же, социальные сети продолжают вытеснять привычные поисковые системы, ведь здесь человек может узнать сразу отзывы других пользователей о товаре или услуге.

В Республике Беларусь существует две группы поставщиков услуг мобильного маркетинга: специализированные маркетинговые агентства (например, компания *Streamline Ltd* и нон-маркетинговые компании, которые предоставляют коммерческое пространство в пределах своих мобильных платформ и приложений. На сегодняшний день белорусская индустрия мобильного маркетинга все еще является недостаточно зрелой. Несмотря на успешность, существует несколько внешних факторов, тормозящих развитие мобильного маркетинга в Республике Беларусь: отсутствие законодательства, регулирующего сегмент мобильного маркетинга, а также зачастую нежелание руководства компаний выделять бюджет на более современные маркетинговые инструменты.

Кроме того, большинство руководителей организаций Республики Беларусь связывают маркетинг лишь с рекламой. Хотя на самом деле маркетинг подразумевает еще много всего, но реклама – это очень важный аспект.

Реклама – это лишь вид маркетинга, это именно то, что позволяет потребителю узнать о товаре. Можно создать просто потрясающий продукт, но его никто не будет покупать, если не будет о нем знать. А любое распространение информации о товаре – это уже реклама, это уже маркетинг. Даже устная информация, советы ваших знакомых и отзывы покупателей в интернете – это тоже вид маркетинга, называемый «сарафанным». Без рекламы бизнес, вряд ли, приносил бы прибыль. Поэтому, использовать ее нужно обязательно. Именно по этой причине, большинство предприятий Минска выделяют часть бюджета на маркетинг, в том числе и рекламу. В связи с развивающимся бизнесом, малым и большим, развивается конкуренция, а, следовательно, каждое предприятие хочет укрепить свою позицию на рынке. Как раз тогда на помощь и приходит маркетинг.

Сейчас в Минске, как и в остальных городах Белоруссии, проходит множество курсов и тренингов, где рассказывают о пользе маркетинга и, что самое главное, как им оперировать в своем бизнесе. Такие знания потом можно удачно использовать для продвижения товара и максимизации прибыли.

**Заключение**

Маркетинг в современном обществе – это «коробка» возможностей. Правильное их использование дает потрясающий результат, а если действовать неверно, или вовсе не действовать, то конкурентные позиции будут очень слабыми. Положение усугубляется постоянным усилением конкурентной борьбы, особенно с зарубежными производителями. Это требует от белорусских отечественных предприятий быстрого и адекватного реагирования на изменение конъюнктуры рынка. Поэтому существует реальная необходимость создания и внедрения механизмов управления, позволяющих воспринимать эти изменения, распознавать их и обеспечивать соответствующую адаптацию производственно-коммерческой деятельности предприятия к рыночным условиям на принципах менеджмента, логистики и маркетинга.

Для соответствия современному уровню рыночных отношений требуется перестройка системы управления предприятием, которая бы ввела дополнительные элементы в управление, обеспечив системность работы с рынком.

**Литература**

1. Акулич И.Л. Маркетинг: учебник / И.Л. Акулич. – 4-е изд. перераб. – Мн.: Выш. шк., 2005. – 463 с.
2. Багиев Г.Л. Международный маркетинг: учебник / Г.Л. Багиев, Н.К. Моисеева С.В. Никофорова. – СПб: Питер, 2001. – 512 с.
3. Котлер Ф. Основы маркетинга / Ф. Котлер, Г. Амстронг, Дж. Сандерс, В. Вонг; пер. с англ. – 2-е европ. изд. – М.: СПб.: К. Издат. дом «Вильямс», 1999. – 1056 с.
4. Котлер, Ф. Маркетинг менеджмент / Ф. Котлер. – СПб: Питер Ком, 1998. – 896 с.
5. Лизакова Р.А. Основы маркетинга: учеб.пособие. – М-во образов. Респ. Беларусь, Гомел.гос.техн.ун-т. – Гомель: ГГТУ им. П.О. Сухого, 2009. – 174 с.
6. Хойер В. Как делать бизнес в Европе / В. Хойер. – М.: Прогресс, 1990. – 253 с.
7. Хоскинг А. Курс предпринимательства. Практ. пособие /А. Хоскинг; пер. с англ. – М.: Междунар. отношения, 1993. – 352 с.
8. Зиссер Ю.А. Маркетинг on-line: Учеб. пособие / Ю.А. Зиссер. – Мн.: «Издательство Гревцова», 2007.

9. Stuart G., Palmieri P. The mobile marketing roadmap / Greg Stuart – Mobile Marketing Association, 2015.
10. Хохрякова К.А. Мобильный маркетинг как новое направление маркетинговых коммуникаций: публикация / К.А. Хохрякова. – БГУ. – Минск, 2009.
11. Мобильный маркетинг растет и развивается. Только не в Беларуси [Электронный ресурс]. – Режим доступа: http://marketing.by/analitika/mobilnyymarketing-rastet-i-razvivaetsya-tolko-ne-v-belarusi/.
12. Колесная И.Н. Мониторинговые системы как инструментарий оценки маркетингового потенциала компаний // Бухгалтерский учет и анализ, 2021. – № 4. – С. 19-24.
13. Трубицина В.А. Роль маркетинга в деятельности предприятия // Научно-методический электронный журнал «Концепт», 2016. – Т. 34. – С. 245-249. – Режим доступа: http://e-koncept.ru/2016/56771.htm. – Дата доступа: 08.02.2022.
14. Колесная И.Н., Тышлек В.В., Давидович В.А. Оценка эффективности коммерциализации и инструментарий маркетинговых исследований инновационных проектов в Республике Беларусь // Бухгалтерский учет и анализ, 2022. – № 1. – С. 44-49.
15. Колесная И.Н. Устойчивое развитие компаний в условиях инновационной экономики // Проблемы экономики и информационных технологий: сборник тезисов докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18-20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники, Минск. 2020. – С. 68-69.

# СЕТИ И СИСТЕМЫ СВЯЗИ

## ОЦЕНКА ПЕРСПЕКТИВ РАЗВИТИЯ И ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МОБИЛЬНОЙ СВЯЗИ 5-ГО И 6-ГО ПОКОЛЕНИЙ

***Ш.И. Исобоев,*** *Московский технический университет связи и информатики, sheros95@mail.ru;*
***Б.М. Халматов,*** *Московский технический университет связи и информатики, bogdanyegorov@gmail.com;*
***В.А. Коптев,*** *Московский технический университет связи и информатики, yyy.xxx.98@bk.ru.*

***УДК 004.8:621.391***

***Аннотация.*** В данной статье проведен анализ методов искусственного интеллекта, используемых для повышения производительности мобильной связи. Кратко описываются подходы к искусственному интеллекту в мобильной связи, несколько классических его методов и современные подходы с применением в беспроводной связи. Методы включают нечеткую логику, нейронные сети, обучение с подкреплением и методы искусственного интеллекта, реализованные в мобильной связи. Рассматриваются некоторые ключевые или терминологические проблемы между искусственным интеллектом и будущей мобильной связью, не только проблемы поколения 5*G*, но и то, как шестое поколение (6*G*) мобильных сетей будет способствовать обеспечению стабильных сетей и типов услуг на огромных мобильных устройствах и данных.

***Ключевые слова:*** искусственный интеллект; 5*G*; 6*G*; *MIMO*; связь.

## ASSESSMENT OF PROSPECTS FOR THE DEVELOPMENT AND APPLICATION OF ARTIFICIAL INTELLIGENCE IN MOBILE COMMUNICATIONS OF THE 5TH AND 6TH GENERATIONS

***Sheroz Isoboev,*** *Moscow Technical University of Communications and Informatics;*
***Bogdan Khalmatov,*** *Moscow Technical University of Communications and Informatics;*
***Viktor Koptev,*** *Moscow Technical University of Communications and Informatics.*

***Annotation.*** This article analyzes the methods of artificial intelligence used to improve the performance of mobile communications. Approaches to artificial intelligence in mobile communications, several classical methods and modern approaches with application in wireless communications are briefly described. Methods include fuzzy logic, neural networks, reinforcement learning, and artificial intelligence methods implemented in mobile communications. Some key or terminological issues between artificial intelligence and future mobile connectivity, not only the problems of the 5*G* generation, but also how the sixth generation (6*G*) of mobile networks will contribute to providing stable networks and types of services on huge mobile devices and data.

***Keywords:*** artificial intelligence; 5*G*; 6*G*; *MIMO*; communication.

### Введение

Искусственный интеллект (ИИ) – это один из методов адаптации человеческого мозга или мышления, других действий животных, биологических систем и видов. В частности, ИИ в системе мобильной связи играет важную роль,

являясь перспективным способом оптимизации ее производительности. В общем плане методы искусственного интеллекта вносят значительный вклад в динамическую адаптацию мобильной связи в окружающей среде. В настоящее время сложная сетевая инфраструктура нуждается в переходе от традиционных методов эксплуатации и управления к интеллектуальному подходу для снижения неэффективности и расширения [1, 2].

Следующее поколение беспроводных сетей является более сложным и требует больше ресурсов из-за необходимости улучшения требований к обслуживанию с различными устройствами, сложными сетями и различными приложениями [3]. Кроме того, сетевые программисты должны адаптировать систему таким образом, чтобы предоставлять наилучшие и доступные ресурсы для повышения качества обслуживания. ИИ предназначен для создания адаптивной системы, обеспечивающей лучшую производительность системы и окружающей среды. Эпоха больших данных приводит к появлению все более массивных наборов данных, доступных с мобильных или беспроводных систем. Другими словами, применяемый ИИ в мобильной связи обеспечит повышение эффективности систем связи, повышение производительности и повышение ключевых показателей эффективности (*Key Performance Indicator, KPI*). Растущая сетевая инфраструктура и аппаратное обеспечение мобильных устройств и их приложений увеличат потребность в мобильных станциях или увеличат объемы мобильного трафика и объем обрабатываемых данных.

**Проблемы искусственного интеллекта в мобильной связи**

ИИ будет играть важную роль в управлении большими данными в качестве передовой аналитики данных и организации различных коммуникационных устройств в будущих мобильных или беспроводных сетях [4]. С другой стороны, инфраструктура мобильной связи должна быть адаптивной к разнообразным услугам, эффективной и надежной. А именно, способствовать повышению производительности мобильной широкополосной связи, минимизации отношения пиковой мощности к средней (*Peak-to-Average-Power-Ratio, PAPR*), улучшению множественного доступа с ортогональным разделением частот (*Orthogonal frequency-division multiplexing, OFDM),* улучшению качества связи.

Другими проблемами ИИ в системе мобильной связи являются принятие решений, управление сетью и оптимизация ресурсов. Что касается мобильной интеллектуальной связи, то она характеризуется проактивной системой, самосознающей, самоадаптивной, прогнозирующей, эффективной и экономичной эксплуатацией и оптимизацией. Еще одним важным аспектом мобильной связи является то, как ИИ может быть применен к различным сценариям беспроводной связи, таким как управление питанием, управление радиоресурсами, управление мобильной связью и управление помехами [5].

**Подход и применение искусственного интеллекта в мобильной связи**

Существует несколько классических подходов к ИИ, таких как нечеткая логика и нейронная сеть. Затем нейронная сеть будет расширена, чтобы использовать более эффективные методы, такие как машинное обучение и подходы к глубокому обучению. Основным подходом является нечеткая логика, в которой обрабатываются любые значения и в результате получаются значения *true* и *false*. Другой термин в ИИ – это обучение с подкреплением, метод проектирования компьютера или машины для самостоятельного обучения вместо того, чтобы быть точно запрограммированным. Одним из методов являются нейронные сети. Эта

техника может быть выполнена с помощью машины или компьютера, способного к самообучению для решения проблемы. Этот процесс перенимает систему и поведение человеческого мозга. В текущих выпусках также было популярно глубокое обучение как улучшенное машинное обучение. Глубокое машинное обучение является интересным подходом для расширенного сетевого трафика и управления будущей мобильной связью. В мобильной связи используются два типа обучения с использованием искусственного интеллекта: обучение под наблюдением и обучение без присмотра.

**Принятие решений в области мобильной связи**

При принятии решений ИИ в мобильной связи необходимо не только количество, но и качество опыта для различных типов услуг с использованием подхода нейронной сети, а также нейронная сеть для классификации ключевых показателей эффективности, объединяющих показатели эффективности с качеством опыта в услугах мобильного интернета.

В общем случае в качестве «помощника» ИИ по поиску контента предлагают качество опыта персонализированной службы поиска контента, которая разделена на два раздела:

1) Точный, чтобы уловить интерес и опыт пользователей.

2) Процесс доступа к удобству и подходящим рекомендациям.

Методы анализа данных, машинного обучения и ИИ могут быть использованы в аналоговом, цифровом и гибридном формировании луча для создания оптимальных диаграмм направленности, динамического выбора наиболее подходящего луча и выполнения операции управления лучом.

**Оптимизация ресурсов в мобильной связи**

При оптимизации ресурсов генетические алгоритмы использовались для оптимизации построения многоадресных деревьев мобильных специальных сетей. К этой оптимизации добавляются дополнительные цели, такие как ограниченная сквозная задержка и энергоэффективность. Также нейронные сети и теоретико-множественный метод применяются для решения задачи сокращения *PAPR*, которая используется для онлайн-обучения. Ключевой компонент повышения эффективности оценки канала *OFDM* также может быть решен с помощью методов ИИ.

Рассматривается когнитивная радиосистема с совместным определением спектра, в которой несколько вторичных пользователей сотрудничают для получения надежных результатов определения спектра и обеспечения эффективного и надежного оппортунистического доступа к спектру. Также был предложен метод ИИ для решения проблемы межсотовых помех, которая может оказать негативное влияние на производительность пользователей беспроводной связи в мобильных сетях. Существующие алгоритмы искусственного интеллекта интегрируют графические процессоры (*Graphics processing unit, GPU*) и центральные процессоры (*Central processing unit, CPU*) для повышения производительности в периферийных вычислениях [6]. Прикладной ИИ для мобильной связи связан со сложными статистическими методами и должен учитывать устройства, инфраструктуру, конечных пользователей, технологии и другие ресурсы.

**Сетевое управление в мобильной связи**

Примером приложения для управления сетью в беспроводной связи является маршрутизация, тема в разделе коммуникации. В некоторых исследованиях уже реализован ИИ для этой темы. Например, применяется нейронная сеть для реализации самонастройки и самооптимизации как для радиоресурса, так и для маршрутизации [7]. В других исследованиях методы машинного обучения использовались для решения различных типов проблем маршрутизации в прошлом. Он содержал маршрутизацию по кратчайшему пути, адаптивную маршрутизацию и многоадресную маршрутизацию. Другой способ управления сетями в беспроводной связи заключается в мониторинге различных сетевых действий и обнаружении аномалий, т.е. событий, которые отклоняются от текущего поведения сети. ИИ также использовался для прогнозирования трафика в сети связи [8]. Технологии ИИ могут свести к минимуму традиционные вмешательства в управление сетевым трафиком и обеспечить надежность, более адаптивные системы и более высокую производительность сети.

**Другие приложения искусственного интеллекта**

В целом, методы искусственного интеллекта, применяемые в мобильной связи, можно увидеть в табл. 1.

Таблица 1.

| **Технология мобильной связи** | **Приложение ИИ** |
|---|---|
| Автономные транспортные средства и устройства для оказания медицинской помощи | • Автоматизация с присущим ей искусственным интеллектом.<br>• Современные и основные алгоритмы в конкретной области искусственного интеллекта для автономных транспортных средств. Такие системы особенно подходят для принятия решений на высоком уровне, поскольку они, по определению, должны быть способны воспринимать окружающую среду и реагировать на нее для достижения поставленных целей. |
| Интернет умных вещей | Методы искусственного интеллекта, используемые для создания такого интеллекта, и сетевые решения для использования преимуществ, приносимых этой возможностью. |
| Мобильные облачные вычисления | Ресурсоемкие приложения, такие как дополненная реальность, искусственный интеллект, искусственное зрение, отслеживание объектов, обработка изображений и обработка естественного языка, становятся популярными для управления мобильными облачными вычисления. |
| Сети 5*G* | Искусственный интеллект и его подкатегории, такие как машинное обучение и глубокое обучение, развиваются как дисциплина до такой степени, что в настоящее время этот механизм позволяет беспроводным сетям пятого поколения (5*G*) быть прогнозирующими и упреждающими, что имеет важное значение для реализации концепции 5*G*. |

| Технология мобильной связи | Приложение ИИ |
|---|---|
| Сети беспроводных сенсоров | • Для оказания помощи интеллектуальным радиоканалам используются инструменты искусственного интеллекта. Инструмент, называемый машинным обучением, считается важным инструментом в решении вышеуказанной проблемы.<br>• Методы машинного обучения для локализации в *WSNS* с использованием индикатора уровня принимаемого сигнала. |
| Мобильные гетерогенные сети (*HetNets*) | Машинное обучение, алгоритмы, вдохновленные биологией, нечеткие нейронные сети и так далее, потому что методы искусственного интеллекта естественным образом могут решать проблемы крупномасштабных сложных систем. |
| Выявление скрытых коммуникаций мобильных вредоносных программ | Для обнаружения вредоносных программ, тайно обменивающихся данными, используются два метода обнаружения, основанных на инструментах искусственного интеллекта, таких как нейронные сети и деревья решений. |
| Мобильные и беспроводные сети | Глубокое обучение. |
| Автомобильные мобильные сети | Кэширование границ на основе искусственного интеллекта. |
| Беспроводные сети нового поколения | Машинное обучение, искусственные нейронные сети.<br>Аналитика больших данных для анализа активности пользователей и обнаружения пользовательских аномалий. |
| Мобильные мультимедиа | Глубокое обучение стало важнейшей технологией для мультимедийных вычислений. |
| Система определения местоположения в помещении на основе *Wi-Fi* | Искусственные нейронные сети. |
| Когнитивные радиосети | Разработка протоколов когнитивной маршрутизации, предусмотренных как протоколы маршрутизации, которые полностью включают в свою разработку методы, основанные на искусственном интеллекте. |
| Наука о данных и искусственный интеллект для коммуникаций | Инновации в области искусственного интеллекта, машинного обучения и анализа сетевых данных предоставляют огромные возможности для революционизации мировых коммуникационных систем и пользовательского опыта. |
| Системы сотовой сети | Концепция искусственного интеллекта и обзор его применения в проектировании, эксплуатации и оптимизации сотовых сетей. |

**Заключение**

ИИ играет важную роль в повышении производительности системы мобильной связи: упреждающая система, самосознательная, самоадаптивная, прогнозирующая, эффективная и экономичная эксплуатация и оптимизация. Было рассмотрено, а также проанализировано несколько классических методов ИИ и современных подходов к ИИ в беспроводной связи. Методы включают нечеткую логику, нейронные сети, обучение с подкреплением и некоторые методы ИИ, реализованные в мобильной связи. Некоторые ключевые проблемы между ИИ и будущей мобильной связью заключаются в том, как управлять, например, большими данными, аналитикой данных, а также передачей на более высоких частотах, связью между устройствами, надежной архитектурой, сверхплотной сетью, массивным *MIMO*, 3*D*-формированием луча, *V*2*X, mm-wave, Cloud-RAN*. Проблемы заключаются в проблемах поколения 5*G* и в том, как поколение 6*G* мобильных сетей будет использоваться для обеспечения стабильных сетей и типов услуг на огромных мобильных устройствах и данных.

**Литература**

1. Клаусманн Л., Ревиллауд М., Глейзер С., Груйер Д. «Исследование подходов на основе искусственного интеллекта для принятия решений на высоком уровне при автономном вождении на шоссе», в 2017 году Международная конференция IEEE по системам, человеку и кибернетике, SMC. 2017.
2. Атов И., Чен К.С. и С.Ю. «Наука о данных и искусственный интеллект для коммуникаций», май, 2019. – Т. 57. – № 5. – С. 56.
3. Болябкин М.В. Интеллектуальная система для преобразования запросов на естественном языке в SQL и их выполнения // Международный журнал гуманитарных и естественных наук, 2021. – № 12-1 (63). – С. 134-138. DOI 10.24412/2500-1000-2021-12-1-134-138.
4. Зюзин В.Д. Инновации на рынке телекоммуникационных услуг // Международный журнал гуманитарных и естественных наук, 2020. – № 8 (47). – С. 143-147. DOI 10.24411/2500-1000-2020-10949.
5. Колесников Р.А., Зюзин В.Д. Проблема электромагнитной совместимости. Электромагнитная обстановка и анализ источников помех для оборудования связи // Инновации и инвестиции, 2020. – № 10. – С. 154-158.
6. Зюзин В.Д. Особенности изучения элементов CPU-логики в рамках курса «сетевые технологии» // Методические вопросы преподавания инфокоммуникаций в высшей школе, 2020. – Т. 9. – № 4. – С. 53-62.
7. Muzata A. R., Pershina V.A. The Modeling of Elastic Traffic Transmisson by the Mobile Network with NB-IoT Functionality // 2021 Systems of Signals Generating and Processing in the Field of on-Board Communications, Conference Proceedings, Moscow, 16-18 марта 2021 года. – Moscow. 2021. – P. 9416132.
8. Артвел Р.М. Анализ принципов функционирования технологии Nb-IOT на основе сетей мобильной связи последних поколений // Телекоммуникационные и вычислительные системы 2020: Труды международной научно-технической конференции, Москва, 14-17 декабря 2020 года / Московский технический университет связи и информатики. – Москва: Научно-техническое издательство «Горячая линия-Телеком», 2020. – С. 183-188.

# АРХИТЕКТУРА HR И LBO РОУМИНГА В СЕТЯХ 5G

***И.А. Михайлова,*** *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, bella300598@mail.ru.*

***УДК 004.428.4***

***Аннотация***. В статье представлен обзор архитектуры роуминга 5*GS* в 3*GPP Release* 16, рассмотрены особенности 5*G* роуминга. Представлены различные аспекты роуминга, которые необходимо учитывать в базовой сети, в области пользовательских данных и в серверных системах. При переходе на 5*G*, услуги, требующие глобального покрытия, лучше всего поддерживаются путем взаимодействия между 5*GC* (5*G Core*) и существующим *Evolved Packet Core* (*EPC*).

***Ключевые слова****:* 5*GS*; 5*GC*; роуминг; *EPC*; *LBO*; *PLMN*; *SEPP*.

# ARCHITECTURE OF HR AND LBO ROAMING IN 5G NETWORKS

***I.A. Mikhailova****, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

***Annotation*.** The article provides an overview of the 5*GS* roaming architecture in 3*GPP* Release 16, and discusses the features of 5*G* roaming. Various aspects of roaming that need to be considered in the core network, in the user data domain and in server systems are presented. In the transition to 5*G*, services requiring global coverage are best supported through interoperability between 5*GC* (5*G Core*) and the existing Evolved Packet Core (*EPC*).

***Keywords:*** 5*GS*; 5*GC*; roaming; *EPC*; *LBO*; *PLMN*; *SEPP.*

## Введение

Цель роуминга – обеспечить беспрепятственное подключение мобильных пользователей к сети, где бы они ни находились. Это имело место для каждого поколения технологий беспроводной связи, но по мере того, как операторы запускают свои коммерческие услуги 5*G*, роуминг становится все более сложным.

Роуминг расширяет покрытие услуг домашнего оператора, позволяя его мобильным пользователям использовать эти услуги в сети другого оператора, в другой стране или в той же стране.

Взаимодействие между 5*GC* и *Evolved Packet Core* (*EPC*) при роуминге имеет решающее значение, поскольку при переходе на 5*G* создается покрытие *NR*. А услуги, требующие широкого покрытия, лучше всего поддерживаются за счет взаимодействия между сетями 5*GC* (5*G Core Network*) и существующим *EPC* [1].

## Архитектура роуминга

Не автономными (*Non Standalone, NSA*) сетями развертывание *EPC* уже было модернизировано для ранней поддержки 5*G NR* при роуминге. В 5*GS* (5*G System*) реализована автономная (*Standalone*, *SA*) поддержка *NR* в *RAN* (*Radio Access Network*) следующего поколения (*next generation, NG-RAN*) и новом ядре 5*GC* [2].

Домашняя маршрутизация (*Home routing, HR*) – основное решение в предоставлении услуг передачи речи в роуминге, которое также будет использоваться и для роуминга 5*GS* (5*G System*).

Роуминг 5*G*, сервисная архитектура (*Service-Based Architecture, SBA*) и функции безопасности являются новыми в 5*GS*, поддерживаемыми новой сетевой

функцией (*Network Function, NF*), называемой прокси-сервером защиты границы безопасности (*Security Edge Protection Proxy, SEPP*).

На рис. 1 показана архитектура роуминга, включающая взаимодействие с *EPS*. Эта архитектура поддерживает роуминг с использованием 5*G* в посещаемой (*Visited Public Land Mobile Network, VPLMN*) и домашней сети мобильной связи общего пользования (*Home Public Land Mobile Network, HPLMN*). Она основана на предположении, что взаимодействие с *EPS* (*Evolved Packet System* (*Core*)) потребуется на начальных этапах роуминга.

Архитектура, показанная на рис. 1, требует, чтобы *UE* мог использовать как *EPS*, так и 5*GS*, чтобы иметь возможность перемещаться между ними. Та же архитектура в *HPLMN* (*Home PLMN*) может также использоваться для *UE* 4*G/NSA* и для *UE*, которым не разрешено использовать 5*GS* в роуминге, но в этих случаях в *VPLMN* будет использоваться только *EPS*. На рис. 1 показана архитектура роуминга с домашней маршрутизацией для взаимодействия между 5*GS* и *EPC/E-UTRAN.*

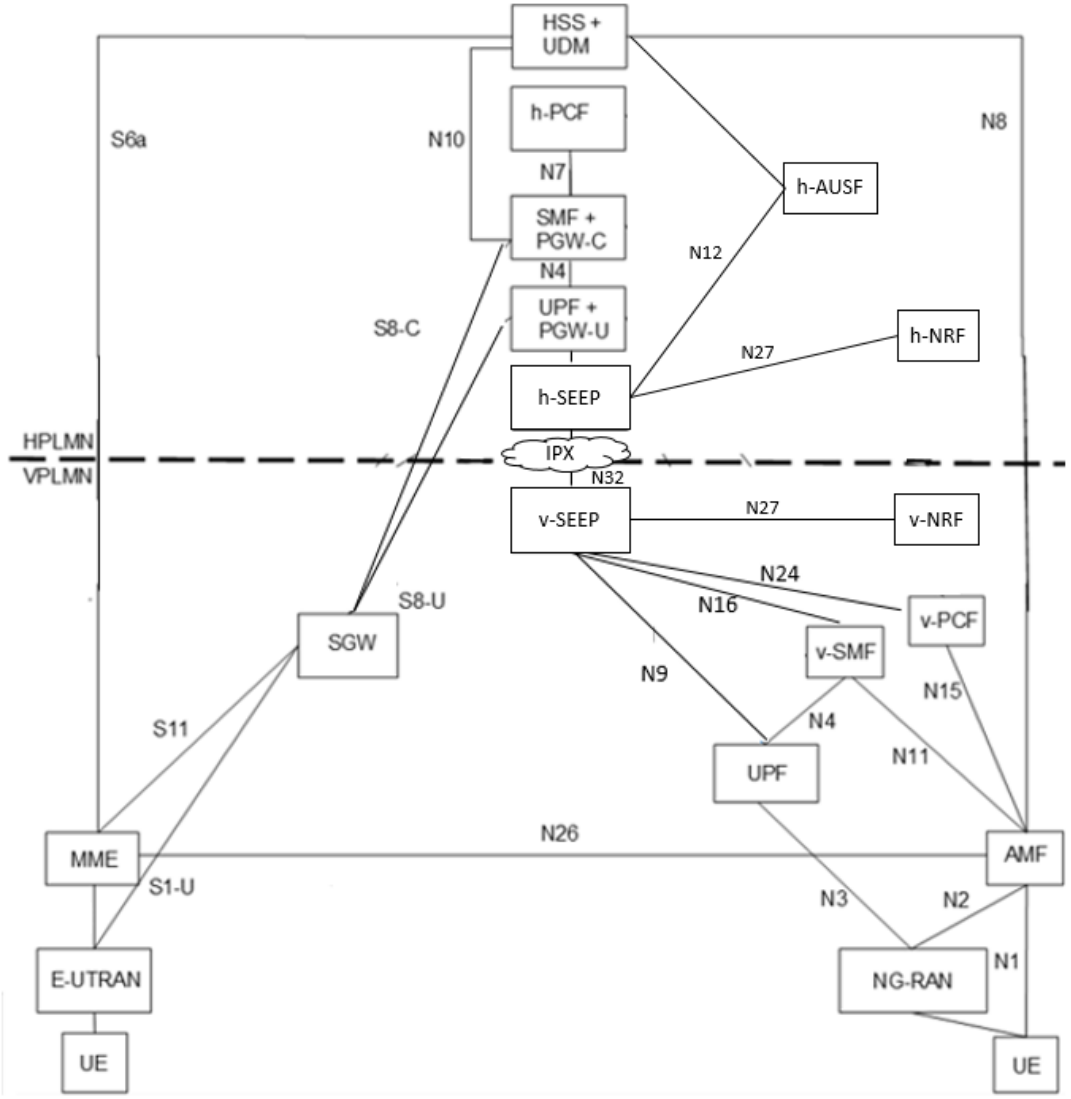



Рисунок 1

Для роуминга в *SBA* (*Service Based Architecture*), *SEPP* обеспечивает передачу сигналов через границы *PLMN,* передавая запросы и ответы для *PLMN,* обеспечивая скрытие топологии, сигнальный *firewall,* фильтрацию сообщений и

дополнительные возможности применения политики. Каждое сообщение плоскости управления в межплатформенной сигнализации передается как по *hSEEP,* так и *vSEPPs PLMN*. Таким образом, *SEPP* может обеспечить защиту сообщений перед отправкой их во внешнюю сеть, а также проверять сообщения, полученные из-за пределов их собственной сети, прежде чем пересылать их в соответствующий *NFs* или прокси-сервер служебной связи (*Service Communication Proxy, SCP*).

*SEPP* будет действовать как непрозрачный прокси-сервер для *NF*, когда сервисные интерфейсы используются в *PLMN,* однако внутри поставщиков услуг *IPX* (*Internet packet Exchange*), а при использовании *HTTP*-прокси также может использоваться для изменения информационных элементов (*IE*) внутри *HTTP*2 сообщения запроса и ответа. Действуя аналогично диаметральному прокси-серверу *IPX*, используемому в роуминге *EPC*, прокси-сервер *HTTP*2 можно использовать для проверки сообщений и изменения параметров. На рис. 2 показана сквозная архитектура на основе служб *HTTP*2, в которой функции прокси-сервера *HTTP* реализуются с помощью *IPX*. *SEPP* потребителя (*consumer cSEPP*) находится в *PLMN*, где находится *NF* потребителя услуг. *SEPP* производителя (*producer pSEPP*) находится в *PLMN*, где находится *NF* поставщика услуг. На рис. 2 показана сквозная архитектура роуминга *HTTP*/2.

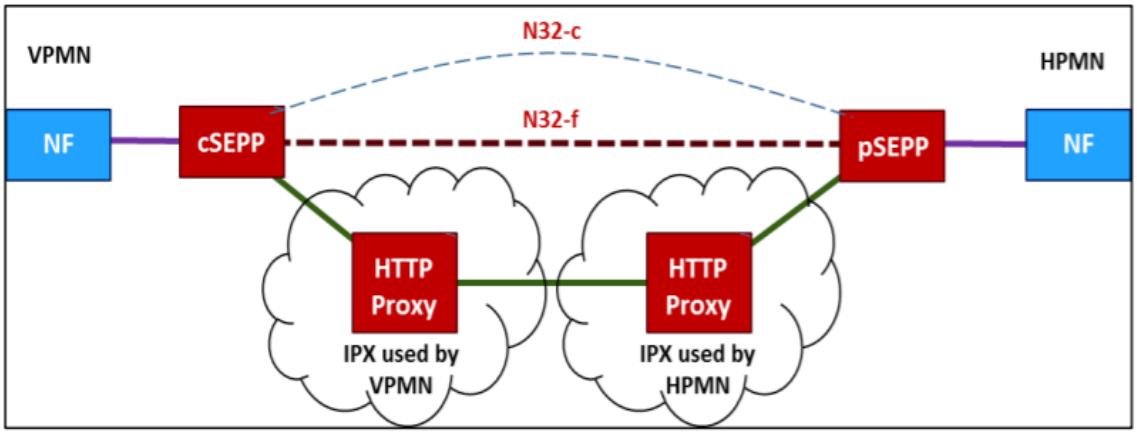



Рисунок 2

*SCP* (*Service Communication Proxy*) был введен в 5*GS* для косвенной связи между *NFs*. *SCP* обеспечивает централизованный мониторинг, защиту от перегрузки и функцию балансировки нагрузки. Кроме того, он обеспечивает унифицированную логику маршрутизации и выбора при определении *NF* назначения или *SCP* следующего перехода. Маршрутизация через *SCP* требует поддержки заголовка 3*gpp-Sbi-Target-apiRoot* для указания целевого назначения *NF*. Принимающий *SEPP* может переслать сообщение непосредственно в конечный *NF* или через *SCP* следующего перехода. Аналогичным образом, когда используется косвенная связь, *SCP* может поддерживать маршрутизацию между *PLMN*, предоставляя логику, необходимую для централизованной маршрутизации соответствующих сообщений в *SEPP.* Каждый оператор может принять решение о развертывании *SCPS* или нет, независимо от решения о поддержке роуминга [3].

Сценарий *Home Routed* (*HR*) использует как *SMF* (*Session Management Function*), так и *UPF* в визитной и домашней сети. В этом случае *SMF* в *HPLMN* (*H-SMF*) выбирает *UPF* в *HPLMN,* а *SMF* в *VPLMN* выбирает *UPF* в *VPLMN*. И *V-SMF*, и *H-SMF* выбираются *AMF* во время установления сеанса *PDU* (*Protocol Data Unit*).

*V-SMF* может быть изменен, например, во время процедуры передачи обслуживания *N*2.

Эталонная точка *N*9 для трафика плоскости пользователя применима только к сценарию *HR*, как показано на рис. 1. Использование *UPF* в *VPLMN* обеспечивает тарификацию *VPLMN, LI VPLMN* и минимизирует влияние на *HPLMN UE.*

Использование *SMF* и *UPF* в *VPLMN* обеспечивает тарификацию *VPLMN*, *VPLMN* и сводит к минимуму влияние на *HPLMN* мобильности *UE* внутри *VPLMN.*

*HPLMN* может управлять с помощью данных подписки на *DNN* (имя сети передачи данных) и на *SNSSAI* (*Single Network Slice Selection Assistance Information)* (информация о помощи при выборе одного сегмента сети) [4].

Процедуры, в случае сеансов *PDU* при развертывании *HR,* характеризуются следующим:

- Управление сеансом *NAS* завершается в *V-SMF* в *VPLMN*.
- *V-SMF* пересылает *H-SMF* информацию, относящуюся к *HPLMN SM*.
- *H-SMF* получает *SUPI* (*Subscriber Permanent Identifier*) *UE* от *V-SMF* во время процедуры установления сеанса *PDU.*
- *H-SMF* отвечает за проверку запроса *UE* в отношении подписки пользователя и за отклонение запроса *UE* в случае несоответствия. *H-SMF* получает данные о подписке непосредственно из *HPLMN UDM* (унифицированное управление данными).
- *H-SMF* может отправлять требования *QoS*, связанные с сеансом *PDU*, в *VSMF*. Это может произойти во время процедуры установления сеанса *PDU* и после установления сеанса *PDU.* Интерфейс между *H-SMF* и *V-SMF* также используется для переноса (*N*9) информации о переадресации плоскости пользователя, которой обмениваются *H-SMF* и *V-SMF*. *V-SMF* может проверять запросы *QoS* от *H-SMF* в отношении соглашений о роуминге.

В случае *HR*-роуминга *AMF* (функция управления доступом и мобильностью) выбирает как *V-SMF*, так и *H-SMF* и предоставляет идентификатор выбранного *H-SMF* в выбранный *V-SMF*.

Отличительной особенностью роуминга 5*GS* является функциональность, подразделяемая на семь областей:

1. Контроль аутентификации со стороны домашней сети.

5*GC* повышает контроль выполнения процедуры аутентификации *UE* в *HPLMN*, так как аутентификация *UE* всегда выполняется и контролируется в *AUSF* (*Authentication Server Function)* на *HPLMN*. Кроме того, *AUSF* информирует модель *UDM* о результате каждой процедуры проверки подлинности *UE*, чтобы модель *UDM* могла связать результат проверки подлинности с последующими процедурами. Это полезно для предотвращения определенных видов мошенничества, таких как мошеннические запросы на регистрацию обслуживающего *AMF* в *UDM* для абонентов, которые фактически не присутствуют (то есть не аутентифицированы) в *VPLMN.*

2. Контроль ограничения роуминга в *HPLMN.*

Когда *UE* с поддержкой 5*GS* пытается подключиться к 5*GC* в роуминге, *VPLMN* запрашивает *HPLMN* авторизацию входящего роуминга абонента для подключения из *VPLMN* до того, как *VPLMN* позволит *UE* подключиться к своим 5*GC*.

*UDM* в пределах 5*GC* на *HPLMN* определяет, разрешено ли *UE* перемещаться в *VPLMN* 5*GC*. Даже если *UE* разрешено перемещаться в *VPLMN* 5*GC*, ограничения роуминга на уровне *UE* могут указывать, какие услуги *HPLMN*

можно использовать во время роуминга (например, службы передачи данных, но не голосовые службы). Если это используется для ограничения голосовой службы *IP Multimedia Subsystem* (*IMS*) в роуминге, голосовой *UE* не будет подключаться к 5*GC* и вместо этого будет искать другой радиодоступ в *VPLMN*, который предоставляет голосовую услугу.

3. Функция управления политиками (*Policy Control Function, PCF*).

Архитектура домашнего роуминга привязывает сеансы *PDU* в *H-SMF*, поэтому для политик управления сеансами все взаимодействия с *PCF* происходят в *HPLMN*.

3*GPP* определяет роли *V-PCF* и *H-PCF*, которые взаимодействуют через интерфейс *N*24 для обмена политиками *UE*, а также политики доступа и мобильности пользователей роуминга.

4. *Charging Function* (*CHF*).

*V-UPF* (*Visited User-Plane Function*) и *H-UPF* (*home-UPF*) должны поддерживать передачу данных сеанса, связанных с *CHF*, в *SMF*, но основная логика *CHF* находится в *SMF*. Как *V-SMF*, так и *H-SMF* должны поддерживать *CHF. V-CHF* генерирует *CDR* (*Call Detail Record*) для входящего роуминг трафика, и, соответственно, *H-CHF* генерирует записи сведений о вызовах (*CDR*) для исходящего трафика роумера.

В результате *VPLMN* имеет полный контроль над объемами данных, которые входящий роумер потребляет в *VPLMN RAN*.

5. Контроль *QoS* (*Quality of Service*) в *V-SMF.*

В сценариях роуминга все параметры *QoS*, запрашиваемые *HPLMN*, должны соответствовать соглашению о роуминге. Однако, чтобы защитить свою сеть от нежелательного использования ресурсов, *VPLMN* должен иметь контроль и, при необходимости, понижение запрошенного *QoS* [5]. 5*GS* вводит четкое разделение между управлением мобильностью (*AMF*) и управлением сеансами (*SMF*), требует, чтобы *V-SMF* обрабатывал управление *QoS*.

6. *Network Slicing* в роуминге.

При регистрации в *AMF UE* определяет сетевые фрагменты, которые он хочет использовать в виде списка сведений о помощи в выборе односетевых фрагментов (*Single Network Slice Selection Assistance Information, S-NSSAI*). *AMF* получает список подписанных *S-NSSAI* от *UDM* в *HPLMN* и определяет какой *S-NSSAI* разрешено использовать *UE.*

*UE* использует разрешенный *NSSAI*, чтобы определить какой *S-NSSAI* использовать при установлении сеанса *PDU*. В простейшем случае в разрешенном *NSSAI* имеется только один *S-NSSAI.* Если это так, *UE* может включить этот *S-NSSAI* при создании сеанса *PDU*, а *AMF* использует этот *S-NSSAI* для выбора *V-SMF* и *H-SMF.* Если в разрешенном *NSSAI* имеется более одного *S-NSSAI*, *UE* нуждается в дополнительной информации о том какой *S-NSSAI* использовать при установлении сеанса *PDU*. Эта дополнительная информация может быть предварительно настроена в *UE* или может быть предоставлена *HPLMN*. Для последнего была указана политика выбора маршрутов *UE*, которая при необходимости может быть предоставлена *H-PCF* (через *V-PCF* и *AMF*) в *UE*. В этом случае требуется опорная точка *N*24 [6].

7. *Steering of Roaming* (Управление роумингом).

Одна из новых функций, определенных для сценариев роуминга 5*GS*, связана с выбором *PLMN* в *UE* во время роуминга. Управление роумингом (*Steering of Roaming, SoR*) в 5*GS* – это решение плоскости управления, которое позволяет *HPLMN* обновлять *UE* списком предпочтительных комбинаций *PLMN/access-*

технологий. *UE* выполняет выбор *PLMN* на основе полученного списка предпочтительных комбинаций *PLMN*/технологии доступа. В предыдущих поколениях список предпочтительных комбинаций *PLMN*/технологии доступа предоставлялся *UE* через механизмы передачи *Over-the-Air* (*OTA*), которые могли быть перехвачены и заблокированы вредоносными *VPLMN* без ведома *HPLMN*.

***LBO* роуминг**

3*GPP* также определил архитектуру локального приземления трафика (*Local Breakout*, *LBO*) в роуминге для предоставления абоненту услуг передачи данных гостевой сетью без привлечения к этому процессу домашней сети. *LBO* не используется для передачи голоса. Следует отметить, что для роуминга требуется, чтобы пользовательское оборудование (*UE*) поддерживало некоторые или все полосы частот, используемые в *VPLMN* (*Visited Public Land Mobile Network*) – не только для *NR*, но и для *LTE* [3]. На рис. 3 показана архитектура системного роуминга 5*G* (*LBO*).

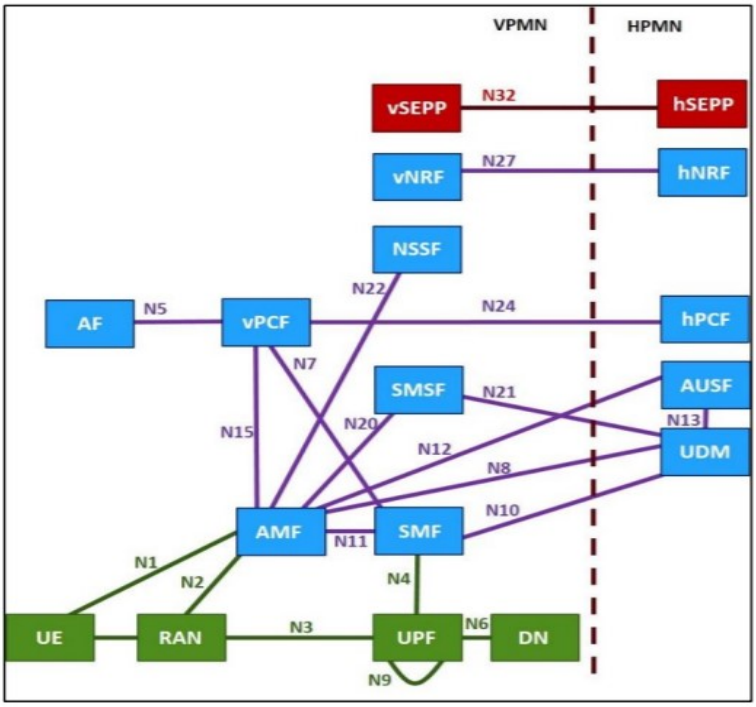



Рисунок 3

Методология выбора *UPF* в *VPLMN* указана в 3*GPP TS* 23.501 [7]. Для сценария развертывания *Local Break Out* (*LBO*) как *SMF* (функция управления сеансом), так и все *UPF* для сеансов *PDU* (блок данных протокола) находятся под управлением *VPLMN*. Подобно случаю без роуминга, *AMF* предоставляет *SMF* в *VPLMN* информацию о местоположении *UE*, а *SMF* в *VPLMN* может выбрать во время установления сеанса *PDU UPF* в граничном местоположении, близком к местоположению *UE*. Если местоположение *UE* изменяется, *SMF* в *VPLMN* может, например:

- Сохранить привязку *UPF* и вставить или перераспределить *I-UPF*.
- Инициировать повторное установление сеанса *PDU* или освободить сеанс *PDU* после процедуры передачи обслуживания [4].

При роуминге с *LBO AMF* выбирает *SMF* в *VPLMN*, как описано в 3*GPP TS* 23.502 [8]. В этом случае при обработке сообщения запроса на установление сеанса

*PDU* функция *SMF* в *VPLMN* может отклонить сообщение, связанное с запросом на установление сеанса *PDU* с надлежащей причиной. Это инициирует *AMF* для выбора как нового *SMF* в *VPLMN*. На рис. 4 показан выбор *SMF* для сценариев *LBO* роуминга.

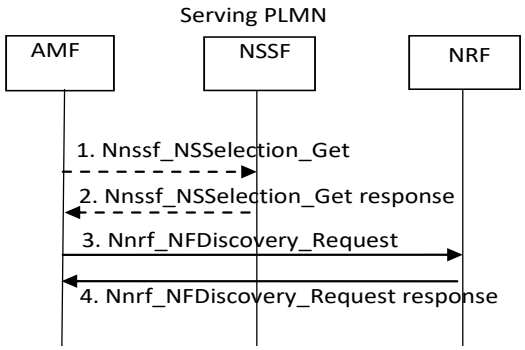



Рисунок 4

Процедура выбора *SMF* доступна в *AMF*:

1. *AMF* вызывает служебную операцию *Nnssf_NSSelection_Get* из *NSSF* в обслуживающей *PLMN*.

2. *NSSF* при обслуживании *PLMN* выбирает экземпляр *Network Slice*, определяет и возвращает соответствующий *NRF*, который будет использоваться для выбора *NF*/услуг в выбранном экземпляре *Network Slice.*

3. *AMF* запрашивает соответствующий *NRF* в обслуживающей *PLMN,* отправляя запрос *Nnrf_NFDiscovery_Request.*

4. *NRF* при обслуживании *PLMN* предоставляет *AMF,* полное доменное имя или *IP*-адрес набора обнаруженных экземпляров *SMF* или адресов конечных точек экземпляров службы *SMF* в ответном сообщении *Nnrf_NFDiscovery_Request* и идентификатор *NSI* для выбранного экземпляра *Network Slice*, соответствующий *S-NSSAI* для последующих запросов *NRF* [8].

**Процедура подключения к сети, установление соединения между *VPLMN-HPLMN***

Без прямого соглашения о роуминге от *HPLMN*, *VPLMN* должна блокировать доступ входящих абонентов в роуминге к своей сети доступа 5*G-NR*. Это обязательно для обеспечения того, чтобы роумеры не столкнулись с какими-либо перебоями в обслуживании, поскольку необходимые технические требования не были реализованы и протестированы в рамках *HPLMN.*

*AMF* в *VPLMN* должен реализовать такую же функцию управления доступом, которая существует в *EPC MME*. Один из механизмов для достижения этого основан на информации о диапазоне *MCC* и *MNC* внутри скрытого идентификатора подписки, *SUCI* (на основе *IMSI*). Используя этот механизм, абонент либо отклоняется с соответствующей причиной отклонения, либо ему разрешается зарегистрироваться [9].

- Причина 15 (отсутствие подходящих сот в зоне отслеживания). Если *VPLMN* уже имеет соглашение о роуминге с *HPLMN,* охватывающее другие технологии радиодоступа (*Radio Access Technologies, RAT*), это вынуждает *UE* повторно выбрать другую *RAT* в той же *PLMN.*
- Причина 11 (*PLMN* не разрешена), если у *VPLMN* нет соглашения о роуминге с *HPLMN*. Это заставляет *UE* выполнять повторный выбор *PLMN*. *UE* должно сохранить идентификатор *PLMN* в «списке запрещенных *PLMN*» в *USIM* (*Universal Subscriber Identity Module*). *UE* больше не должно пытаться

выбрать этот *PLMN*. Также можно использовать причину 13 (чтобы избежать постоянного хранения *PLMN* в файле *Forbidden PLMN* в *USIM*).

Если *VPLMN* не реализует эти требования, то *HPLMN* может реализовать свою собственную функцию управления доступом в *UDM* для защиты своих подписчиков. Если у *HPLMN* уже есть соглашение о роуминге с *VPLMN*, охватывающее другие технологии доступа *RAT*, то индикация отклонения, отправленная *UDM* обратно в *AMF* в ответе *Nudm_UECM_Registration* с кодом состояния *HTTP* «403 *Forbidden*», будет содержать дополнительную информацию об ошибке в ответе, элемент «*ProblemDetails*». Тип данных «*ProblemDetails*» будет использовать атрибут «*cause*» Выбор *SMF* для сценариев *LBO* роуминга *RAT_NOT_ALLOWED*. Рис. 5 показана регистрация *AMF* и оказание услуг подключения [10].

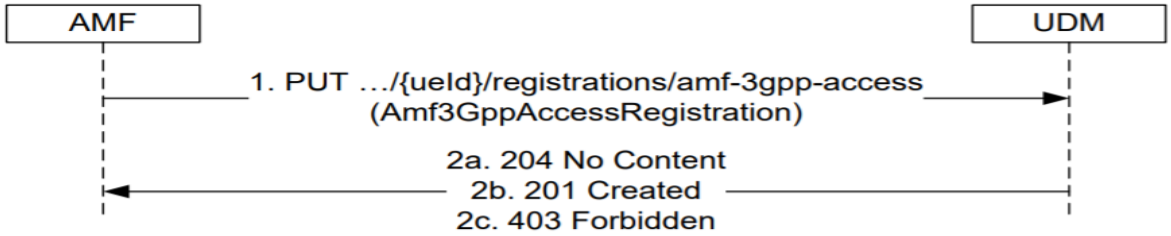



Рисунок 5

Затем *AMF* должен преобразовать причину *RAT_NOT_ALLOWED* из *UDM* в причине 15 (нет подходящих сот в области отслеживания) для отправки в *UE*. *AMF* не должен сопоставлять *RAT_NOT_ALLOWED*, причиной 12 (область отслеживания не разрешена), причиной 13 (роуминг в этой области отслеживания не разрешен) или причиной 11 (*PLMN* не разрешен) [4].

Когда *UE* подключается к *VPLMN*, он регистрируется в функции управления доступом и мобильностью (*Access and Mobility Management Function*, *AMF*). *AMF* будет запрашивать функцию сетевого репозитория (*Network Repository Function, NRF*), которая в данном случае служит в качестве посещаемого *NRF* (*V-NRF*), а *V-NRF* будет запрашивать домашнюю *NRF* (*H-NRF*), чтобы найти функцию сервера аутентификации (*Authentication Server Function*, *AUSF*) и унифицированное управление данными (*Unified Data Management, UDM*) в *HPLMN*. Как трафик между *V-NRF* и *H-NRF*, так и весь другой трафик плоскости управления между *VPLMN* и *HPLMN* будут проходить через *SEPP*, что можно заметить на рис. 6.

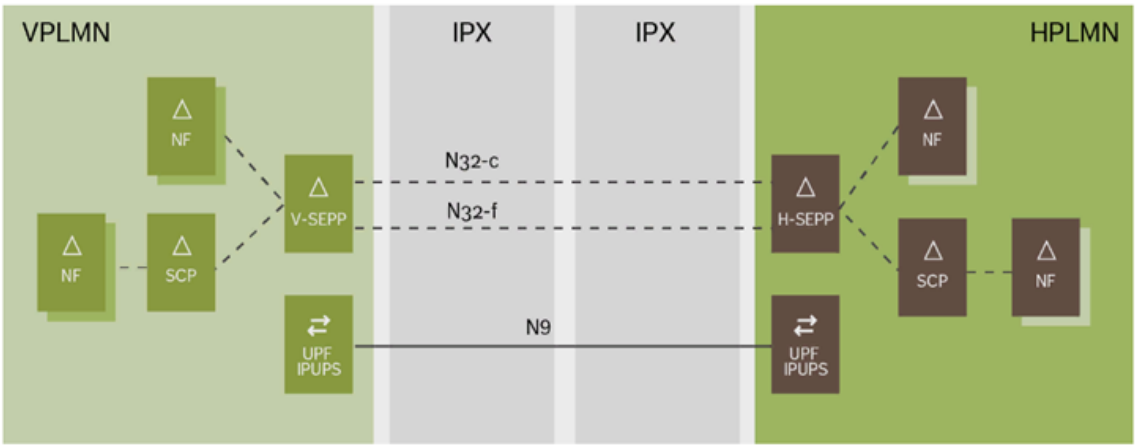



Рисунок 6

*UE* устанавливает один или несколько сеансов данных протокола (*Protocol Data Unit, PDU*). Использование функции управления сеансами (*V-SMF*) при мобильности характерны для роуминга, то есть *V-SMF* используется только тогда, когда *UE* находится в *VPLMN,* а сеанс *PDU* привязан к домашней *SMF* (*Session Management Function, H-SMF*) в *HPLMN*. В роуминге *EPS* узлы *EPC*, обслуживающие шлюз (*Serving Gateway, SGW*) и шлюз пакетной сети передачи данных (*Packet Data Network Gateway, PDN-GW*), используются в соединении *PDN*, независимо от того, находится ли *UE* в *VPLMN* или *HPLMN* [11].

Соединение между *SEPP VPLMN* и *HPLMN* в сценариях роуминга использует интерфейс *N*32. *3GPP* определил *N*32 как два отдельных интерфейса: *N*32-*c* и *N*32-*f*. *N*32-*c* – это интерфейс *Control Plane* между *SEPP* для выполнения согласования параметров, которые должны применяться для фактической пересылки сообщений *N*32. Как только соединение *HTTP*2 завершено, соединение *N*32-*c* разрывается, рис. 7. Это соединение является сквозным между *SEPP* и не использует *IPX* для перехвата соединения *HTTP*2, но *IPX* может быть задействован для маршрутизации на уровне *IP* [12]. На рис. 7 показан интерфейс *N*32-*c*.

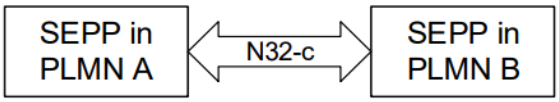



Рисунок 7

*N*32-*f* – это интерфейс пересылки между *SEPP*, который используется для переадресации связи между потребителем услуги сетевой функции (*NF*) и производителем услуги *NF* после применения защиты безопасности на уровне приложения. *N*32-*f* может обеспечить безопасность на уровне приложений (*Application Level Security, ALS*), между *SEPP*, если согласовано с использованием *N*32-*c*, рис. 8 [13]. На рис. 8 показан интерфейс *N*32-*f*.

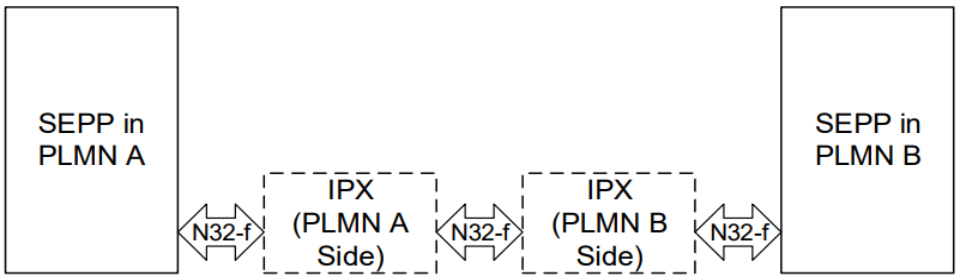



Рисунок 8

Рис. 6 показывает *IPX* (обмена интернет-протоколами) между *VPLMN* и *HPLMN*, но также возможное наличие только одного или даже отсутствие *IPX* (например, в случае национального роуминга).

*SEPPs* аутентифицируются с использованием протокола безопасности транспортного уровня (*TLS*) через интерфейс плоскости управления *N*32 (*N*32-*c*), а также с использованием протокола *TLS* для защиты сообщений через интерфейс пересылки *N*32 (*N*32-*f*). Каждый *SEPP* должен иметь учетные данные *SEPP* партнера по роумингу. Для предоставления так называемых услуг с добавленной стоимостью в роуминге 3*GPP* также стандартизировал *PRINS* (Протокол для обеспечения безопасности соединений *N*32) по *N*32-*f*, чтобы *IPX* мог добавлять модификации определенных элементов сообщений, сохраняя при этом исходные элементы. Даже если только одной стороне требуется его функциональность,

*PRINS* требует поддержки как *VPLMN*, так и *HPLMN*, что означает, что они оба должны принять сложность, которую *PRINS* вводит для контрактов, эксплуатации и безопасности [14].

В то время как *SEPP* обеспечивает безопасность сообщений уровня управления, защита сообщений уровня пользователя в связи между *PLMN* обеспечивается функциями безопасности уровня пользователя между *PLMN* (*IPUPS*) в существующих *UPFS,* которые управляются *V-SMF* и *H-SMF*, как показано на рис. 6. *IPUPS* защищает трафик *GTP-U* (*Tunneling Protocol GPRS-User*), перенаправляя только допустимый трафик через опорную точку *N*9 между *PLMN* и отбрасывая оставшийся недопустимый трафик.

*SEPP* в *PLMN* должен содержать управляемую оператором политику, которая указывает, какие *IE* могут быть изменены провайдером *IPX*, непосредственно связанным с конкретным *SEPP*. Например, «*SUPI*, постоянный идентификатор абонента» или «данные о местоположении».

Как указано в 3*GPP TS* 33.501 [13], каждый *PLMN* должен согласовать политику модификации с провайдером *IPX*, с которым он связан до установления соединения *N*32. Каждая политика модификации применяется к одному отдельному отношению между оператором *PLMN* и провайдером *IPX*. Для охвата полного соединения *N*32 оба вовлеченных партнера по роумингу должны обменяться своими политиками модификации. Обе дополнительные политики модификации должны включать общую политику модификации для этого конкретного соединения *N*32.

Для проверки изменений сообщений, полученных через интерфейс *N*32-*f*, партнеры оператора по роумингу должны знать общую политику модификации. Модификация включает в себя удаление и добавление нового *IE* (*Information Element*). Поэтому *IE* могут отсутствовать в переписанном сообщении.

*IE,* которые разрешено изменять *IPX*, должны быть указаны в списке, дающем перечисление путей *JSON* (*JavaScript Object Notation*) в объекте *JSON*, созданном *SEPP*. Подстановочные знаки могут использоваться для указания путей.

Эта политика должна быть специфичной для каждого партнера по роумингу и для каждого провайдера *IPX*, используемого для конкретного партнера по роумингу.

Политика модификации должна находиться в *SEPP*. Для каждого партнера по роумингу *SEPP* должна иметь возможность хранить политику для отправки в дополнение к политике для получения [15].

Следующее основное правило проверки всегда должно применяться независимо от политики, которой обмениваются два партнера по роумингу: *IE*, требующий шифрования, не должен быть вставлен в другое место в объекте *JSON* [4].

**Заключение**

Одним из основных преимуществ архитектуры роуминга 5*GS* является возможность расширения существующего роумингового решения *EPS* за счет использования 5*GS* в *VPLMN* и мобильности между 5*GS* и *EPS* при роуминге. Пользовательское оборудование, способное использовать как *EPS*, так и 5*GS*, также сможет использовать как *EPS*, так и 5*GS* роуминг.

Внедрение роуминга 5*GS* потребует внимания во всех доменах. Существуют аспекты роуминга, которые необходимо учитывать в основной сети, в пользовательских данных и политиках, в службах и в серверных системах. В тоже

время необходимо обеспечить безопасность партнеров по роумингу. К счастью, все эти аспекты рассмотрены в выпуске 16 3*GPP* новой базовой линии для роуминга.

**Литература**


1. 5G migration strategy from EPS to 5G system [Электронный ресурс] URL: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/migration-from-eps-to-5gs (дата обращения – февраль 2022 г.).
2. Ericsson Technology Review, 5G migration strategy from EPS to 5G system [Электронный ресурс] URL: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-ran-and-transport-choices-that-minimize-tco (дата обращения – февраль 2022 г.).
3. Roaming in the 5G System: the 5GS roaming architecture [Электронный ресурс] URL:https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/roaming-in-the-5g-system (дата обращения – февраль 2022 г.).
4. 5GS Roaming Guidelines [Электронный ресурс] URL: https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v5.0-2.pdf (дата обращения – февраль 2022 г.).
5. NG.113 5GS Roaming Guidelines v5.0, 16 декабря 2019 г. [Электронный ресурс] URL: https://www.gsma.com/newsroom/resources/ng-113-5gs-roaming-guidelines-v5-0/ (дата обращения – февраль 2022 г.).
6. Roaming in the 5G System: the 5GS roaming architecture [Электронный ресурс] URL: https://www.ericsson.com (дата обращения – февраль 2022 г.).
7. 3GPP TS 23.501 [Электронный ресурс] URL: https://portal.3gpp.org (дата обращения – февраль 2022 г.).
8. 3GPP TS 23.502 [Электронный ресурс] URL: https://portal.3gpp.org (дата обращения – февраль 2022 г.).
9. 3GPP TS 24.501 [Электронный ресурс] URL: https://portal.3gpp.org (дата обращения – февраль 2022 г.).
10. 3GPP TS 38.801 NR [Электронный ресурс]. URL: https://portal.3gpp.org (дата обращения – февраль 2022 г.).
11. Книга Ericsson 5G RAN System Techniques
12. 3GPP TS 29.573 [Электронный ресурс] URL: https://portal.3gpp.org (дата обращения – февраль 2022 г.).
13. 3GPP TS 33.501 [Электронный ресурс] URL: https://portal.3gpp.org (дата обращения – февраль 2022 г.).
14. 3GPP TS 38.913 NR; [Электронный ресурс]. Directory Listing /ftp/Specs/archive/38_series/38.913/ (3gpp.org) (дата обращения – февраль 2022 г.).
15. Архитектура сети 5G [Электронный ресурс]. https://itechinfo.ru/content/архитектура-сети-5g 1 (дата обращения – февраль 2022 г.).

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## ТЕНДЕНЦИИ РАЗВИТИЯ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ДИНАМИЧЕСКОГО ИЗМЕНЕНИЯ ПАРАДИГМЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

***М.М. Добрышин***, *к.т.н., Академия ФСО России, dobrithin@ya.ru.*

***УДК 004.942***

***Аннотация.*** Совершенствование средств и систем обеспечения информационной безопасности основывается на динамическом изменении теоретического аппарата. Существующие дескриптивный аппарат, законы, аксиоматические ограничения и допущения, принципы и методы требуют дополнения и уточнения из-за динамически изменяющейся парадигмы применения информационно-технического оружия. В статье в обобщенном виде представлены основные элементы теории, сформулированы новые факторы, требующие учета и предложены уточненные принципы обеспечения информационной безопасности.

***Ключевые слова****:* теория информационной безопасности; принцип; информационно-техническое оружие.

## TENDENCIES OF DEVELOPMENT OF THE THEORY OF INFORMATION SECURITY IN THE CONDITIONS OF DYNAMIC CHANGE OF THE PARADIGM OF APPLICATION OF INFORMATION AND TECHNICAL INFLUENCES

***M.M. Dobryshin,*** *Candidate of Technical Science, Academy of the FSO of Russia, employee.*

***Annotation.*** Improvement of means and systems of information security support is based on dynamic change of the theoretical device. The existing descriptive devices, laws, axiomatic restrictions and assumptions, the principles and methods demand addition and specification because of dynamically changing paradigm of use of the information and technical weapon. In article basic elements of the theory are presented in a generalized view, the new factors demanding accounting are formulated and the specified principles of information security support are offered

***Keyword:*** theory of information security; principle; information and technical weapon.

**Введение**

Теория информационной безопасности (ИБ), как и все прикладные области знаний, появилась, формировалась и развивается на основе возникновения противоречий в практике, а именно неудовлетворенностью пользователей сетей связи в защищенности, обрабатываемой, передаваемой и хранимой информации. Наличие инцидентов информационной безопасности вызвано двумя основными факторами, первым является непрерывное стремление злоумышленников достичь своих деструктивных целей (хищение, искажение или блокирование информации) путем использования уязвимостей возникших при синтезе, проектировании, производстве и эксплуатации сетей и средств связи (в том числе упущения при

синтезе систем обеспечения информационной безопасности и комплексном применении группы средств защиты); ко второму следует отнести стремление пользователей применять новые технологии в повседневной деятельности (и как следствие появлению новых уязвимостей), а также их непрерывное перемещение между элементами сети. Указанные факторы выводят применяемые средства защиты и систему обеспечения информационной безопасности в целом из равновесного состояния (определенных условий функционирования), снижают их эффективность и соответственно снижается защищенность [1-3].

Анализ инцидентов информационной безопасности показывает, что существенная их часть вызвана недостаточной проработкой теоретических основ [4-6]. Противоречия в теории возникают из-за появления новых подходов, методов и принципов применения информационно-технического оружия [7], которые в свою очередь вызваны изменением структуры и возможностей компьютерных сетей [8].

**Сущность, понятийно-категорийный аппарат и этапы развития теории информационной безопасности**

Для понимания сущности, содержании основных элементов и этапов развития теории, проведен анализ ряда работ по философии [9-14], который позволил определить ее основные элементы и в обобщенном виде схему их взаимосвязи (рис. 1). На рис. 1 показана концептуальная схема взаимосвязи элементов, образующих научную теорию.

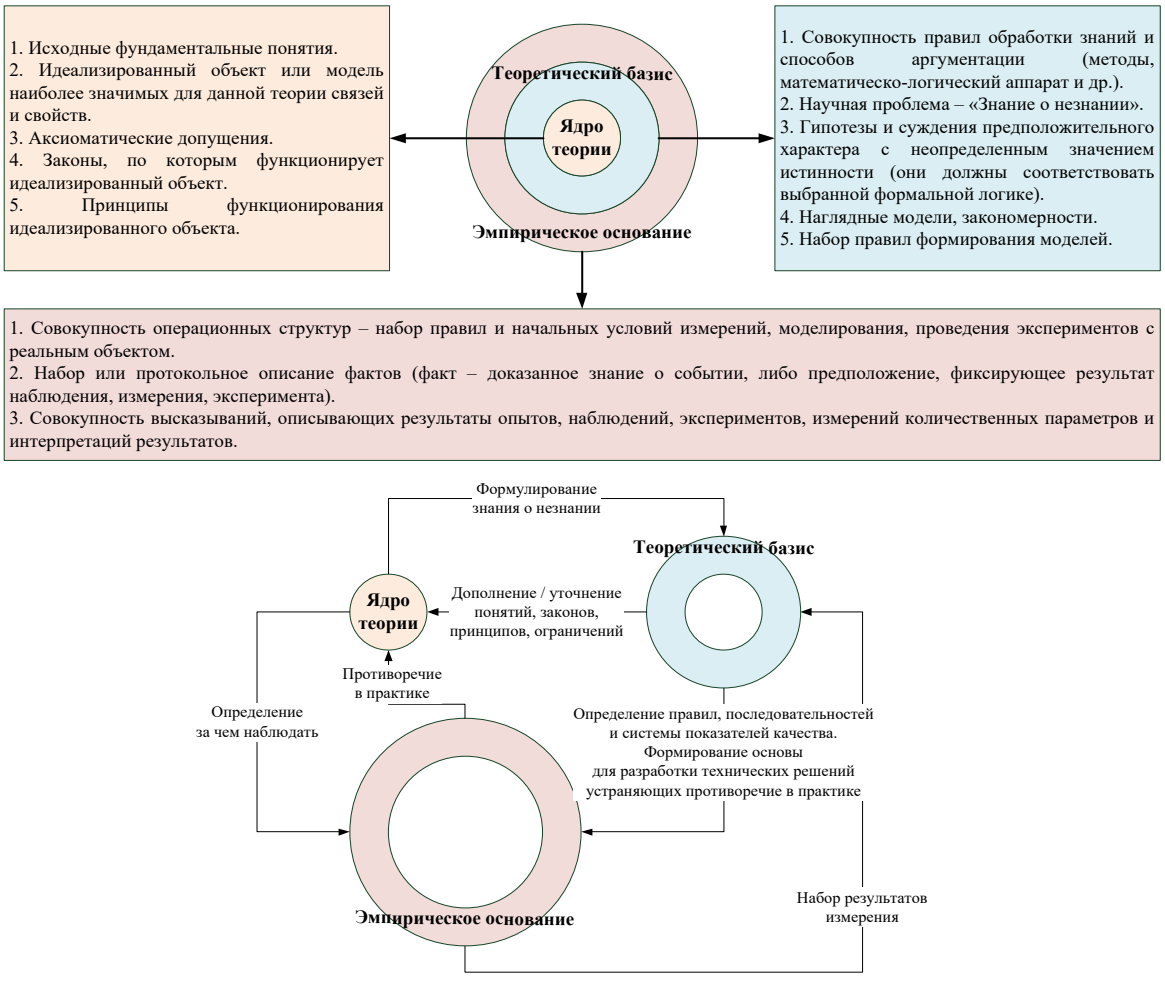



Рисунок 1

Основу теории ИБ составляет понятийно-категорийный аппарат (в том числе совокупность аксиоматических ограничений и допущений), законы, принципы и правила. Концептуальная схема позволила сформулировать последовательность развития теории информационной безопасности (рис. 2). Учитывая, что законы информационной безопасности (законы Индюкова, Митника, Склярова, Батенева, Дейкстры и др.) [15] носят системообразующий характер и не зависят от изменения внешних воздействий, а понятийно-категорийный аппарат отражает объекты защиты, основными объектами теории, подверженными изменению во времени, являются принципы и методы. На рис. 2 показан вариант последовательности развития теории информационной безопасности.

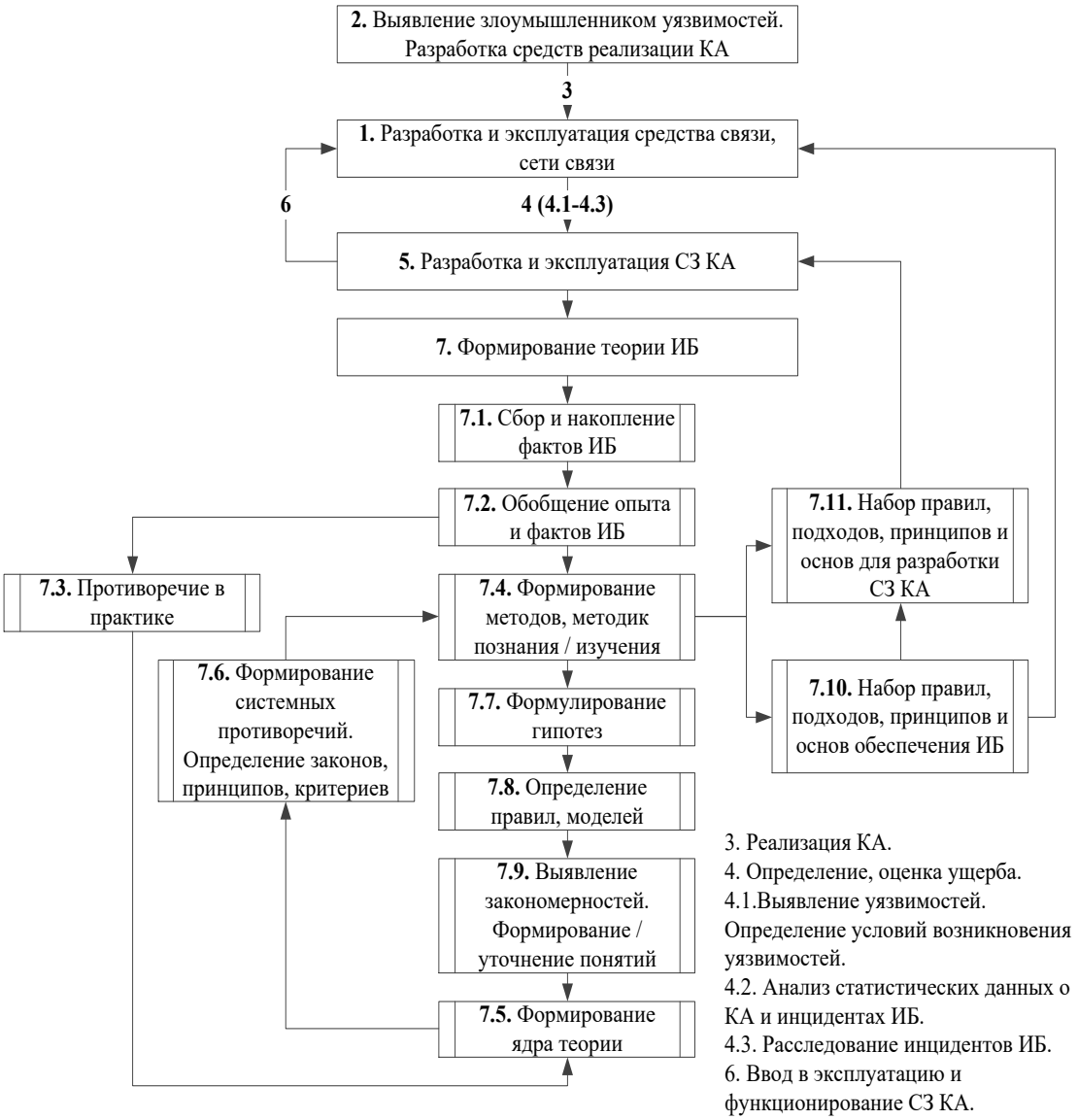



Рисунок 2

Процесс обеспечения информационной безопасности целесообразно разделить на два основных подпроцесса [1, 16]:

- подпроцесс синтеза средств и систем обеспечения информационной безопасности (на данном этапе задаются и воспроизводятся основные свойства и возможности – тактико-технические характеристики);
- подпроцесс динамической защиты средств обработки, хранения и передачи информации, а также элементов и сети связи в целом (выявление событий ИБ, противодействие фактам информационной безопасности и минимизация ущерба, ликвидация последствий, проведение расследований инцидентов).

Основываясь на том, что основные требования, предъявляемые к системе обеспечения информационной безопасности задаются на этапе ее синтеза и уточняются в ходе ее эксплуатации [1], очевидно, что основным объектом совершенствования теории является уточнение и развитие *принципов синтеза* (проектирования) систем обеспечения информационной безопасности. В настоящее время основными принципами являются [6, 17, 18]: концептуальное единство; адекватность требованиям; гибкость (адаптируемость); функциональная самостоятельность; удобство использования; минимизация предоставляемых прав; полнота контроля; экономичность.

Под *концептуальным единством* понимается идеологически общая архитектура, технология, организация и обеспечение функционирования системы и ее элементов.

Принцип *адекватности требованиям* – система строится в строгом соответствии с требованиями к защите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

*Гибкость* (*адаптируемость*) системы – такое построение и такая организация ее функционирования, при которых функции защиты осуществляются эффективно при изменении в некотором диапазоне структуры сети связи, технологических схем или условий функционирования каких-либо ее элементов.

*Функциональная самостоятельность* – система должна быть самостоятельно обеспечивающей подсистемой сети связи и при осуществлении функций защиты не зависеть от других подсистем.

*Удобство* использования означает, что система обеспечения информационной безопасности не должна создавать дополнительные неудобства пользователям и персоналу сети связи.

*Минимизация предоставляемых прав* – каждому пользователю предоставляются лишь те полномочия на доступ к ресурсам сети и находящейся в ней информации, которые ему необходимы для выполнения своих обязанностей.

*Полнота контроля* – все процедуры обработки защищаемой информации должны контролироваться системой защиты в полном объеме, основные результаты контроля должны фиксироваться в регистрационных журналах.

*Активность реагирования* – система должна реагировать на любые попытки несанкционированных действий.

*Экономичность* – расходы на эксплуатацию системы должны быть минимальными.

Однако, непрерывный рост ущерба от различных видов компьютерных атак, свидетельствует о том, что применяемые технические решения недостаточно эффективны, что в свою очередь вызвано недостаточной адаптацией теоретического аппарата к следующим изменившимся условиям и дестабилизирующим факторам:

1. Применяемые при синтезе средств и систем обеспечения информационной безопасности, модели угроз информационной безопасности носят статичный характер, однако статистические данные и проводимые ранее исследования свидетельствуют о динамичном изменении этих угроз, как следствие вводимые в эксплуатацию системы недостаточно эффективны.

2. Модель угроз информационной безопасности сети связи носит статичный характер, однако в ходе эксплуатации сети связи появляются новые элементы сети, сервисы или услуги связи, которые ранее не применялись, что приводит к возникновению новых угроз, которые ранее не были учтены.

3. Перемещение абонентов сети между элементами (узлами) сети приводит к изменению направлений информационных потоков, важности этих элементов (важность элемента определяется категорией важности абонентов, объемом информационных потоков и количеством предоставляемых услуг связи) и как следствие возникновению новых угроз информационной безопасности, защиту от которых применяемая система обеспечения информационной безопасности не гарантирует.

4. Модернизация системы обеспечения информационной безопасности заключается в вводе в эксплуатацию дополнительных средств или обновлении имеющихся, не учитывая их взаимного влияния и влияние на качество предоставляемых абонентам услуг связи.

5. Рассмотрение системы обеспечения информационной безопасности, как совокупности средств защиты, без учета взаимного влияния друг на друга и качество предоставляемых услуг связи приводит к ее эффективности или снижению качества предоставляемых услуг связи.

6. Использование новых сервисов и услуг связи, программного обеспечения и протоколов сетевого взаимодействия требует применения дополнительных средств мониторинга, защиты и аудита информационной безопасности и как следствие необходимости разработки новых метрик оценки уровня информационной безопасности и адаптации алгоритмов управления.

7. Расширение возможностей средств и способов применения компьютерных атак требует повышения быстродействия системы обеспечения информационной безопасности, однако применяемая метрика оценки ущерба носит эвристический характер и не позволяет своевременно реагировать на выявленные факты инцидентов информационной безопасности.

8. Появление новых и изменение известных видов компьютерных атак требует модернизировать систему обеспечения информационной безопасности в ходе ее эксплуатации, но технические возможности позволяют это сделать не в полной мере.

9. Одним из объектов воздействий является непосредственно система обеспечения информационной безопасности, целью воздействия является как нарушение ее функционирования, так и вывод ее в режимы работы, затрудняющие процесс предоставления услуг связи абонентам.

Для устранения выявленных противоречий, повышения уровня защищенности сети, основываясь на результатах проведенных ранее работ в предметной области [1, 3, 16-22] и исходя из логики развития теории (рис. 2) предлагается уточнить (дополнить) известные принципы следующим образом:

Принцип концептуального единства, с учетом указанных противоречий дополнить и считать его *принципом целостности системы* обеспечения информационной безопасности – понимается идеологически общая архитектура, технология, организация и обеспечение функционирования системы и ее

элементов, позволяющая применение новых элементов и обеспечивающая усиление (не снижение) положительных свойств элементов, не вызывая при этом затруднений в реализации услуг связи.

*Принцип адекватности требованиям* (уточненный) – система строится в строгом соответствии с требованиями к защите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации в момент ввода ее в эксплуатацию и изменяющимися соизмеримо возможностям средств и способов воздействия.

Под принципом *адаптируемости системы в условиях нестационарности угроз* следует понимать возможность изменять структуру, технологии анализа и обработки событий ИБ, реагирования на факты ИБ при возникновении новых или улучшении характеристик известных средств и способов реализации угроз ИБ, а также изменения структуры защищаемой сети, использования новых средств и видов связи.

Принцип *функциональной самостоятельности* – система должна быть самостоятельно обеспечивающей подсистемой сети связи, а именно, обеспечивать собственное устойчивое функционирование и при осуществлении функций защиты не зависеть от других подсистем.

Остальные принципы (удобство использования; минимизация предоставляемых прав; полнота контроля; экономичность) исходя из перечисленных противоречий не требуют уточнений.

**Заключение**

Таким образом, на основании общих подходов к формированию научных теорий, произведено структурирование элементов теории информационной безопасности, уточнены ее основные элемента. На основании анализа статистических данных определен перечень противоречий в практике, что позволило с учетом ранее проведенных исследований уточнить известные принципы синтеза систем обеспечения информационной безопасности, которые при их реализации позволят повысить защищенность сетей связи от различных видов информационно-технических воздействий.

**Литература**

1. Белов А.С., Добрышин М.М., Борзова Н.Ю. Формирование модели угроз информационной безопасности на среднесрочный период // Приборы и системы, Управление, контроль, диагностика, 2021. – № 7. – С. 41-48.
2. Добрышин М.М. Методика выбора последовательности применения информационно-технического оружия в отношении компьютерной сети с учетом стратегий распределения ресурсов обороняющейся стороны / Известия Тульского государственного университета. Технические науки, 2020. – № 9. – С. 232-237.
3. Добрышин М.М., Шугуров Д.Е. Иерархическая многоуровневая модель таргетированных компьютерных атак в отношении корпоративных компьютерных сетей / Проблемы информационной безопасности. Компьютерные системы, 2020. – № 4. – С. 35-46.
4. Аникин И.В. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики. Диссертация на соискание ученой степени доктора технических наук. ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» Казань, 2017.

5. Лаврова Д.С. Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции / Диссертация на соискание ученой степени доктора технических наук. ФГАОУ ВО СПбПУ, Санкт-Петербург, 2019.
6. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления / Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с.
7. Добрышин М.М. Особенности применения информационно-технического оружия при ведении современных гибридных войн // I-methods, 2020. – Т. 12. – № 1. – С. 1-11.
8. Добрышин М.М. Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки, 2021. – № 9. – С. 113-121.
9. Никифоров А.Л. Философия науки: история и методология. – М.: 1998, История философии. Запад – Россия – Восток. Кн. 4. – М.: 1999.
10. Степин В.С. Теоретическое знание. Структура, историческая эволюция. – М.: 2000.
11. Кузнецов И.В. Структура научной теории и структура объекта // Вопросы философии, 1968. – № 5. – С. 1-12.
12. Никифоров А.Л. Философия науки: история и методология. – М.: 1998.
13. Пассмор Дж. Сто лет философии. – М.: 1998.
14. Фоллмер Г. Эволюционная теория познания. – М.: 1998.
15. Коробейников А.Г. Теория ИБ и методология защиты информации // ИТМО СПб, 2018. –100 с.
16. Добрышин М.М. Белов А.С., Горшков А.А., Борзова Н.Ю. Предложение по проектированию систем обеспечения информационной безопасности с применением элементов ТРИЗ // Известия Тульского государственного университета. Технические науки, 2021. – № 9. – С. 38-44.
17. Зегжда Д.П. Принципы и методы создания защищенных систем обработки информации: дис. … докт. техн. наук: 05.13.19. – СПб.: Санкт-Петербургский государственный политехнический университет, 2002. – 380 с.
18. Еременко В.Т. Комплексные системы защиты информации предприятия: учебное пособие. – Орел: ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. – 116 с.
19. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.
20. Добрышин М.М., Горшков А.Н., Белов А.С., Борзова Н.Ю. Предложение по проектированию систем обеспечения информационной безопасности с применением элементов ТРИЗ // Известия Тульского государственного университета. Технические науки, 2021. – № 9. – С. 38-44.
21. Смирнов Е.В. Методика оценки политической значимости угроз объекту критической информационной инфраструктуры на примере объекта инфокоммуникаций // Экономика и качество систем связи, 2020. – № 2 (16). – С. 49-56.
22. Смирнов Г.Е., Макаренко С.И. Использование тестовых информационно-технических воздействий для превентивного аудита защищенности информационно-телекоммуникационных сетей // Экономика и качество систем связи, 2020. – № 3 (17). – С. 43-59.

# ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА МОНИТОРИНГА БЕЗОПАСНОСТИ СЕТИ БЕСПРОВОДНОЙ СВЯЗИ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

***Ш.И. Исобоев,*** *Московский технический университет связи и информатики, sheros95@mail.ru;*
***Д.А. Везарко,*** *Московский технический университет связи и информатики, vezarko00@mail.ru;*
***А.С. Чечельницкий,*** *Московский технический университет связи и информатики, mr.vip64@yandex.ru.*

***УДК 004.8:004.056:004.85***

***Аннотация.*** Для решения проблем традиционных систем мониторинга уязвимостей безопасности сетей беспроводной связи, таких как низкая точность мониторинга и трудоемкость, в статье предлагается интеллектуальная система мониторинга уязвимостей на основе машинного обучения. Представлен алгоритм машинного обучения, который сочетается с программным обеспечением интеллектуальной системы мониторинга для реализации интеллектуального мониторинга уязвимостей безопасности сети беспроводной связи. Результаты эксперимента показывают, что интеллектуальная система мониторинга уязвимостей сети беспроводной связи, основанная на машинном обучении, может эффективно повысить точность мониторинга системы и эффективность мониторинга уязвимостей сети беспроводной связи.

***Ключевые слова:*** сеть; связь; система; мониторинг; уязвимость.

# WIRELESS COMMUNICATION NETWORK SECURITY INTELLIGENT MONITORING SYSTEM BASED ON MACHINE LEARNING

***Sheroz Isoboev,*** *Moscow Technical University of Communications and Informatics;*
***Daniil Vezarko,*** *Moscow Technical University of Communications and Informatics;*
***Alexei Chechelnitsky,*** *Moscow Technical University of Communications and Informatics.*

***Annotation.*** The purpose of this article is to find solutions to the problems of traditional wireless network security vulnerability monitoring systems such as low monitoring accuracy and labor intensiveness.
An intelligent vulnerability monitoring system based on machine learning is proposed. A machine learning algorithm that is combined with intelligent monitoring system software to implement intelligent monitoring of wireless network security vulnerabilities is presented. The results of the experiment show that an intelligent wireless network vulnerability monitoring system based on machine learning can effectively improve the accuracy of system monitoring and the effectiveness of wireless network vulnerability monitoring.

***Keywords:*** network; communication; system; monitoring; vulnerability.

## Введение

В связи с быстрым развитием технологий беспроводных сетей крупные сетевые операторы рассматривают развитие сети беспроводной связи как важную цель развития и постоянно увеличивают инвестиции в их развитие [1]. С появлением технологии 5*G* сеть беспроводной связи также достигла значительного

развития, но возникающие в результате этого проблемы безопасности стали предметом исследований в этой области. Безопасность сети беспроводной связи зависит от информационной безопасности общества и даже страны. Среди них уязвимость безопасности сети беспроводной связи стала главной проблемой, которую необходимо решить в настоящее время. Эта проблема приведет к появлению большого количества данных об уязвимостях, которые представляют собой серию данных, генерируемых уязвимостью безопасности в аппаратном обеспечении, программном обеспечении, протоколе или конкретной системе связи. Анализируя данные о месте утечки, можно определить причины ее образования и своевременно устранить, чтобы обеспечить безопасность сети беспроводной связи. Вопрос о том, как улучшить возможности автономной защиты и мониторинга уязвимостей сетевой системы беспроводной связи, стал актуальной проблемой в этой области. По этому вопросу проведено много исследований [2, 3].

В данной статье предлагается разработка интеллектуальной системы мониторинга уязвимостей безопасности сети беспроводной связи на основе машинного обучения. Система внедряет алгоритмы машинного обучения и завершает разработку интеллектуальной системы мониторинга уязвимостей в сети беспроводной связи посредством разработки аппаратного и программного обеспечения [4]. Результаты экспериментов показывают, что система может эффективно отслеживать уязвимости безопасности сетей беспроводной связи с высокой точностью мониторинга и высокой эффективностью работы.

**Проектирование аппаратного обеспечения**

При фактическом развертывании сети беспроводной связи контроллер РТК-5500 устанавливается в пригородной базовой сети для управления платформой и обеспечением безопасности сети беспроводной связи.

Оригинальная система мониторинга уязвимостей безопасности сети беспроводной связи в основном использует технологию *ICMP Echo* и широковещательного сканирования *ICMP* для сканирования уязвимостей сети беспроводной связи. Процесс работы системы заключается в отправке запросов в сеть беспроводной связи и ожидании ответа хоста на мониторинг, а внутренняя структура системы мониторинга сложна. Большая задержка ответа не способствует своевременному мониторингу уязвимостей сети беспроводной связи. Аппаратное обеспечение усовершенствованной системы включает в себя три модуля: модуль сбора данных об уязвимостях, модуль сканирования данных об уязвимостях и модуль интеллектуального мониторинга уязвимостей безопасности беспроводной сети.

Данные об уязвимостях собираются напрямую, а для передачи данных, полученных путем сбора, сканирования и мониторинга, используется технология высокоскоростной передачи данных *t-MPLS*. Технология машинного обучения используется для повышения общей эффективности мониторинга уязвимостей, а машинное обучение используется для сканирования уязвимостей с высокой скоростью для достижения эффективного мониторинга уязвимостей. Улучшенная система мониторинга более чувствительна к реакции мониторинга уязвимостей и снижает затраты на разработку системы.

**Модуль сбора данных об уязвимостях**

Модуль сбора данных об уязвимости безопасности включает в себя:

- Сбор данных об уязвимостях безопасности сетей беспроводной связи.
- Определение уязвимостей беспроводных данных.

- Анализ взаимосвязи между данными.
- Неопределённые уязвимости безопасности при интеграции данных.
- Интегрированный сбор данных об уязвимостях безопасности сети беспроводной связи.

Интерфейс питания сборщика данных имеет тип прямого подключения *DC*12*V*, а сетевой кабель подключается через сетевой порт *RJ*45, и данные с передатчика могут быть перенаправлены на сервер, что удобно и просто в эксплуатации.

**Модуль сканирования данных об уязвимостях**

Система оснащена сканером уязвимостей для бесперебойной работы узлов сети беспроводной связи. Интерфейс сканера уязвимостей классифицирует и сканирует данные узлов сети беспроводной связи, а также собирает различные узлы данных в один и тот же набор для обеспечения безопасности процесса сканирования данных. Подключаемый сканер *XSS* используется для сканирования уязвимостей безопасности сети беспроводной связи.

**Модуль интеллектуального мониторинга уязвимостей беспроводной сети связи в системе безопасности**

При отслеживании сигнала данных об уязвимостях беспроводной сети связи необходимо следить за работой системного сеанса данных об уязвимостях, анализировать информацию об уязвимостях безопасности сети связи в соответствии с различными стандартами заказчика, помечать данные об уязвимостях системы, выбирать разумный режим сопоставления и реорганизовать фрагментацию *IP* сети связи, улучшать производительность системы протоколов высокого уровня, уменьшать сложность поиска пространственных данных, использовать это в качестве основы мониторинга данных об уязвимостях, выбирать информацию о данных, которая не соответствует системе, и объединять их, чтобы сформировать полный набор данных об уязвимостях.

**Разработка системного программного обеспечения**

Чтобы усилить программную часть системы мониторинга, авторами представлен алгоритм машинного обучения, который сочетается с программным обеспечением интеллектуальной системы мониторинга для реализации интеллектуального мониторинга уязвимостей безопасности сети беспроводной связи.

Предполагая, что большая часть последовательности данных, подлежащих тестированию в сети беспроводной связи, представляет собой обычные данные сети беспроводной связи, данные об уязвимостях безопасности становятся объектом системного мониторинга. Обычные данные в сети беспроводной связи обрабатываются с помощью функции оптимальной оценки $F$: $x \to y$, тогда есть $x_i \in X$, $y_i \in Y$, и оптимальная функция оценки может быть выражена следующим образом:

$$F^* = x + \frac{\omega}{n}\sum_{i=1}^{n}\phi(F(c_1)) \tag{1}$$

В формуле $\varphi$ представляет функцию потерь, $\omega$ представляет гармонический параметр данных об уязвимостях безопасности, а $F(cc_1)$ – правило оптимизации.

В процессе мониторинга уязвимостей безопасности сети беспроводной связи функция оптимальной оценки используется для обработки обычных данных

в сети связи. Однако все еще существуют аномальные данные, которые глубоко замаскированы, поэтому требуется их дальнейшая обработка. Необходимо представить алгоритм нейронной сети, отфильтровать его и построить трехслойную модель алгоритма нейронной сети, включающую входной уровень, выходной уровень и уровень правил. Если данные сети беспроводной связи скрыты, выходные данные каждого узла сети связи будут выглядеть так:

$$\begin{aligned}\xi_i^1(c_1) &= v(c_1), i = 1,2,3\cdots n \\ \xi_i^1(c_2) &= v(c_2), i = 1,2,3\cdots n \\ \xi_i^1(c_3) &= v(c_3), i = 1,2,3\cdots n\end{aligned} \tag{2}$$

Приведенные выше три уравнения представляют выходные данные сети связи трехслойной нейронной сети. Вычисление нечеткого выходного значения на каждом уровне происходит следующим образом:

$$\xi_i^4 = \psi_i f_i(rc_1 + rc_2\cdots + rc_n), i = 1,2,3\cdots n \tag{3}$$

В формуле (3), $\psi$ представляет интенсивность нечеткой обработки, а $r$ – коэффициент импульса данных сети беспроводной связи.

**Экспериментальный анализ**

*Экспериментальная среда и настройки параметров*

Эксперимент проводился на платформе *Matlab*, операционной системой была *Windows* 10, процессор *E*52678*V*3.

Содержание параметров эксперимента задается так, как показано в табл. 1.

Таблица 1.

| Параметр | Значение |
|---|---|
| *CPU* / ГГц | 3,4 |
| Роутер | атака роутера |
| Память сервера / ГБ | 8 |
| *IP*-статус данных | обычный |
| Оперативная память | 4 |
| Уязвимые данные / шт. | 100 |
| Обычные данные / шт. | 100 |

*Анализ точности мониторинга уязвимостей*

Чтобы дополнительно проверить эффективность системы, в эксперименте сравнивалась точность трех методов при мониторинге 200 единиц данных беспроводной связи и точность обнаружения утечек данных. Результаты эксперимента приведены в табл. 2.

Анализируя данные, приведенные в табл. 2, можно видеть, что с постоянным увеличением объема данных мониторинга точность мониторинга трех методов имеет тенденцию к снижению. Из табл. 2 следует, что, когда количество объектов данных мониторинга равно 100, точность данных об уязвимостях, отслеживаемых методом, описанным в этой статье, составляет 95%, точность метода, описанного в литературе [2], составляет 85%, а точность метода, описанного в литературе [3], составляет 82%.

Таблица 2.

| Мониторинг данных / шт. | Метод, приведенный в статье (%) | Метод, приведенный в литературе [2] (%) | Метод, приведенный в литературе [3] (%) |
|---|---|---|---|
| 50 | 97 | 92 | 90 |
| 100 | 95 | 85 | 82 |
| 150 | 92 | 80 | 76 |
| 200 | 90 | 78 | 70 |

Когда число объектов данных мониторинга равны 200, точность метода в этой статье составляет 90%, точность метода в литературе [2] составляет 78%, а точность метода в литературе [3] составляет 70%. Хотя точность мониторинга демонстрирует тенденцию к снижению, точность данных об уязвимостях, отслеживаемых предлагаемым методом, превышает 90%, что выше, чем у двух других методов.

**Заключение**

Основываясь на традиционной системе мониторинга уязвимостей безопасности сети беспроводной связи, в данной статье предлагается интеллектуальная система мониторинга уязвимостей безопасности сети беспроводной связи с машинным обучением. Благодаря совершенствованию функций системного аппаратного модуля в сочетании с интеллектуальными алгоритмами машинного обучения, анализом атрибутов данных об уязвимостях безопасности сети беспроводной связи и т.д., была завершена разработка интеллектуальной системы мониторинга уязвимостей безопасности сети беспроводной связи. Результаты экспериментов показывают, что точность мониторинга уязвимостей безопасности в сетях беспроводной связи с использованием этого метода превышает 90%, а эффективность работы высока, что имеет определенное практическое значение в этой области.

**Литература**

1. Зюзин В.Д. Перспективы развития российского информационного общества: уровни цифрового разрыва // Оригинальные исследования, 2020. – Т. 10. – № 8. – С. 123-129.
2. Чжао Юэхуа, Дин Юань Хао. Исследование и внедрение Технологии мониторинга уязвимостей гонки ядра на основе аппаратной виртуализации [J]. Руководство по программному обеспечению, 2015. – № 14 (5). – С. 161-164.
3. Чжан Бинь, Гуанхуй, Чэнь Си. Архитектура безопасности беспроводной ячеистой сети на основе смарт-контракта [J]. Компьютерная инженерия, 2019. – № 45 (11). – С. 16-23, 31.
4. Болябкин М.В. Интеллектуальная система для преобразования запросов на естественном языке в SQL и их выполнения // Международный журнал гуманитарных и естественных наук, 2021. – № 12-1 (63). – С. 134-138. DOI 10.24412/2500-1000-2021-12-1-134-138.
5. Зюзин В.Д. Инновации на рынке телекоммуникационных услуг // Международный журнал гуманитарных и естественных наук, 2020. – № 8 (47). – С. 143-147. DOI 10.24411/2500-1000-2020-10949.

# ПЕДАГОГИКА

## МЕТОДИЧЕСКАЯ СИСТЕМА ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНОЙ КУЛЬТУРЫ БУДУЩИХ ИНЖЕНЕРОВ

***Г.М. Булдык,*** *д.п.н., профессор, Белорусская государственная академия связи, bugemi@mail.ru.*

***УДК 378.02:378.8***

***Аннотация.*** В статье рассматривается методическая система формирования профессиональной культуры инженера, представляющая собой комплекс взаимосвязанных и взаимообусловленных компонентов (содержательного, мотивационно-целевого, процессуального и контрольно-оценочного), объединенных общей стержневой идеей – подготовка высокопрофессионального, творческого и конкурентоспособного специалиста. Именно через профессиональную культуру, представленную ключевыми компетенциями и квалификациями, проявляются цели, мотивы, профессиональные знания, умения, навыки и опыт деятельности, мировоззренческие установки будущего инженера.

***Ключевые слова:*** методическая система; культура; инженер; содержательный компонент; мотивационно-целевой компонент; процессуальный компонент; контрольно-оценочный компонент.

## METHODOLOGICAL SYSTEM FOR FORMING PROFESSIONAL CULTURE OF FUTURE ENGINEERS

***G.M. Buldyk****, doctor of pedagogical sciences, professor, Belarusian State Academy of Communications.*

***Annotation.*** The article discusses a methodological system for the formation of an engineer's professional culture, which is a complex of interrelated and interdependent components (substantive, motivational-targeted, procedural and control-evaluative), united by a common core idea – the preparation of a highly professional, creative and competitive specialist. It is through the professional culture, represented by key competencies and qualifications, that the goals, motives, professional knowledge, abilities, skills and experience, worldview attitudes of the future engineer are manifested.

***Keywords:*** methodological system; culture; engineer; content component; motivational-target component; procedural component; control and evaluation component.

**Введение**

Под методической системой понимается общая направленность обучения. В методической системе методы выступают способами реализации целей и содержания, воплощением психологических механизмов обучения и учения, что упрощает процедуру их выбора. Сегодня в сложившейся социокультурной и экономической ситуации в республике все более значимым становится подготовка высокопрофессионального, творческого и конкурентоспособного инженера. Квалификационные требования к инженеру вышли за пределы профессиональных стандартов и предполагают более широкий спектр знаний, умений, навыков и опыта деятельности, формируемых благодаря образовательному, развивающему и

воспитательному потенциалу учебных дисциплин. Инженер должен уметь анализировать, предвидеть и прогнозировать различные производственные ситуации, уметь принимать правильные решения, быть способным предвидеть конечный результат действий.

Полипарадигмальный подход в процессе подготовки инженеров, при его правильном построении и применении в состоянии реально повысить уровень профессиональной компетентности с помощью различных парадигм, активизируя самообразовательную познавательную деятельность студентов, интегрируя личностно ориентировано-развивающий, компетентностный и деятельностный подходы.

В рамках нашего исследования мы определяем профессиональную культуру инженера как некоторую категорию, имеющую универсальный характер, поскольку она включает в себя профессионализм, мастерство, креативные способности, высокий интеллект и культурно-нравственные ценности личности.

Профессиональная культура представляет собой некий желаемый образ инженера, характеризует типологические особенности, присущие ему как профессионалу и личности, проявляющиеся в личностно-гуманном отношении к действительности в смысловых границах существования специалиста в пространстве профессионального бытия. При проектировании системы формирования профессиональной культуры будущего инженера в техническом университете мы прибегаем к полипарадигмальному подходу, который получает все большее распространение в связи с тем, что образование может быть представлено как в социальном аспекте, так и удовлетворения потребности личности в саморазвитии, самопознании, познании окружающего мира. Благодаря данному подходу мы получаем возможность изучить систему ценностей современного инженера и его заинтересованность в процессе формирования профессиональной культуры [1].

**Методическая система формирования профессиональной культуры студентов инженерных специальностей**

В современной культуре личности выделяются три составляющие: духовные ценности, общение и творческая деятельность. Личность как творец и носитель культуры может характеризоваться с точки зрения ее нравственной культуры и эстетической, меры ее психологической зрелости и интеллектуального развития со стороны ее мировоззренческих позиций. Стержень духовной культуры составляет нравственная культура личности, которая включает в себя культуру человеческого сознания и культуру повседневного поведения. Процесс нравственного формирования личности включает формирование знаний, умений личности в сфере моральной деятельности. Культуру личности можно характеризовать и с точки зрения профессиональной культуры, поскольку ценности являются ядром как общей, так и профессиональной культуры человека. Следовательно, ценностные ориентации будущего инженера на профессиональную культуру, по нашему мнению, это достаточно сложные, определенным образом сгруппированные принципы, придающие целевую направленность различным мотивам и интересам субъекта деятельности в ходе решения различных профессиональных проблем с целью формирования профессиональной культуры.

Культура влияет на поведение, общение, отношение не прямо, а опосредованно − через профессиональные ценности, нормы, роли. Система профессиональных ценностных ориентиров образует пространство развития личности инженера, в поле которого идет присвоение ценностей культуры

профессиональной деятельности. Это означает, что инженер должен не только обладать широким кругозором общих и специальных знаний, но и одновременно быть готовым приобрести новые, чтобы приспособиться к динамично изменяющимся условиям рынка труда. Сформированность этих качеств у современного специалиста служит фундаментом профессиональной культуры. Они открывают возможности для вхождения в поле профессиональной деятельности. Таким образом, в структуре «профессиональная культура инженера» выделяются профессиональные знания, которыми должен владеть специалист (ключевые компетенции), и качественная гуманитарная характеристика профессиональной культуры как часть общей духовной культуры личности (ключевые квалификации) [2].

Разработка методической системы формирования профессиональной культуры базируется на фундаментальных идеях системного подхода в современном научном познании. Под системным подходом понимают методологическое направление в науке, основная задача которого заключается в разработке методов исследования и проектирования сложно организованных объектов – систем разных типов, а под системой – совокупность элементов, находящихся в определенных отношениях друг с другом и со средой. Фундаментальные понятия системного подхода были разработаны в исследованиях А.Н. Аверьянова, В.Г. Афанасьева, Л. Берталанфи, И.В. Блауберга, М.К. Мамардашвили, Б.Н. Кедрова, В.Н. Садовского, Э.Г. Юдина и др.

Если система понимается как совокупность взаимосвязанных элементов, образующих целостность или единство, то структура – это способ взаимодействия элементов системы посредством определенных связей (картина связей и их стабильностей). Изучение структуры той или иной системы имеет принципиальное значение, так как именно способ взаимодействия элементов системы, характер связей и отношений между ее элементами часто определяет отличие этой системы от других систем [3].

Системный подход к педагогическим явлениям рассматривался в работах С.И. Архангельского, В.П. Беспалько, Т.А. Ильиной, Ф.Ф. Королева, Н.В. Кузьминой, И.П. Подласого, Н.Ф. Талызиной и др. Под педагогической системой, согласно Н.В. Кузьминой, понимают «множество взаимосвязанных структурных и функциональных компонентов, подчиненных целям воспитания, образования и обучения подрастающих поколений и взрослых людей». В сходном ключе дают определение педагогической и дидактической систем И.П. Подласый, В.П. Беспалько, В.М. Монахов и др.

Методическая система может быть интерпретирована как проекция дидактической системы обучения на определенную предметную область. Следовательно, методическая система формирования профессиональной культуры инженера может быть рассмотрена как подсистема, компонент общей дидактической системы инженерного образования.

Методическая система формирования профессиональной культуры инженера представляет собой комплекс взаимосвязанных и взаимообусловленных компонентов (мотивационно-целевого, содержательного, процессуального и контрольного), объединенных общей стержневой идеей формирования профессиональной культуры в качестве методической основы процесса обучения.

Качественными характеристиками технологического обеспечения процесса формирования профессиональной культуры будущих инженеров является его направленность на накопление опыта поисковой, эвристической деятельности,

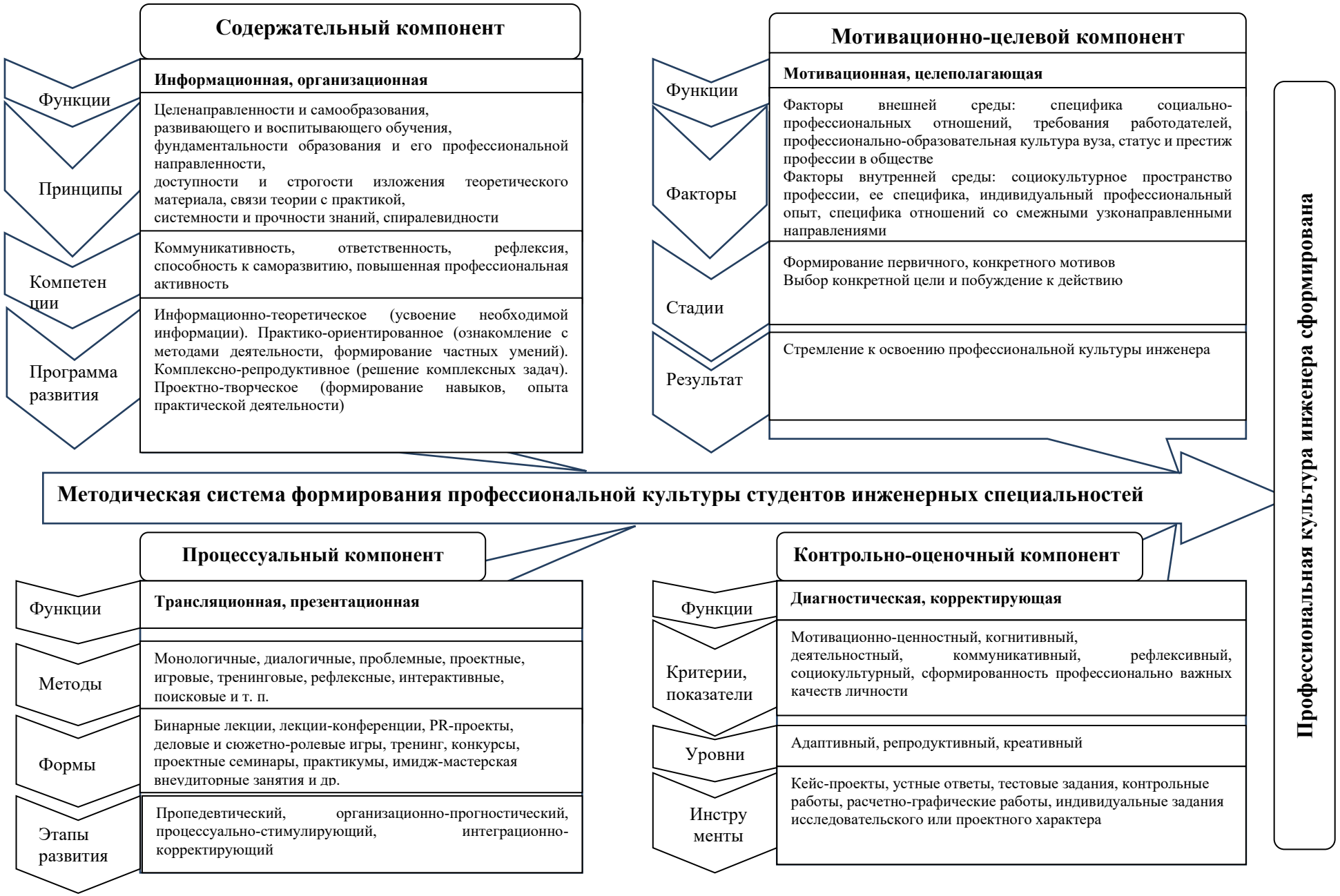
развитие способности видеть и разрешать проблемы, вести диалог, на воспитание профессионально важных личностных качеств.

Структурно-содержательная модель [1], являясь аналогом процесса формирования профессиональной культуры у студентов в системе высшего технического образования, включая такие компоненты, как методологический, содержательный, технологический и оценочно-результативный, а также блок педагогических условий, отражает ведущие характеристики педагогического процесса, способствует отчетливому видению его внутренней структуры, системы влияющих на него факторов, ресурсного обеспечения обучения, позволяет управлять его качеством.

Развитие профессиональной культуры будущих инженеров в вузе определяется рядом условий: это общие, или объективные условия, детерминированные социальным заказом общества, его требованиями к качеству инженерной деятельности; частные условия, связанные с особенностями организации образовательного процесса в вузе, качеством управления учебной деятельностью студентов по овладению инженерной культурой; специфические, или субъективные условия, связанные с субъективными предпосылками успешности будущей профессиональной деятельности, обеспечивающие развитие мотивации, инженерного мышления, рефлексии.

Педагогическое сопровождение формирования профессиональной культуры студентов в образовательном процессе высшей школы строится на основе методологических подходов: системно-деятельностного, компетентностного, личностно-ориентированного. Соответственно, принципами реализации педагогического сопровождения формирования профессиональной культуры будущих инженеров, по нашему мнению, являются: принцип системности, принцип приоритета индивидуальности и самоценности обучаемого, принцип субъект-субъектных отношений педагога и студента, которые реализуются в образовательном процессе посредством использования современных информационно-коммуникационных технологий, направленных на решение образовательных задач. В процессе педагогического сопровождения преподаватель реализует мотивационную, информационную и технологическую функции.

По мнению А.А. Вербицкого, суть мотивационной функции заключается в ориентации мотивационной сферы студентов на задачи личностного самопознания, самоопределения, саморазвития. Реализуя названную функцию, преподаватель помогает студенту осознать потребность в развитии своего творческого потенциала, ориентирует его на творческое саморазвитие. З.А. Исаева определяет, что информационная функция педагогического обеспечения состоит в трансляции студентами знаний о феномене творчества, знаний о собственной индивидуальности, в ознакомлении их со способами осуществления творческой деятельности и приемами творческого саморазвития, а также в адаптации информации для адекватного восприятия ее студентами. Как отмечает М.П. Лапчик, технологическая функция педагогического обеспечения формирования у студентов готовности к творческой самореализации в условиях информатизации образовательного пространства и образовательной среды обучения заключается в предоставлении им необходимых условий и средств для реализации этого процесса. Это обучение студентов умениям и навыкам проектной деятельности, информационных и коммуникационных технологий и программных средств (в том числе мультимедиа) в процессе учебно-познавательной деятельности и в своей жизнедеятельности [4, 5].


Содержательный компонент
Функции
Информационная, организационная
Принципы
Целенаправленности и самообразования, развивающего и воспитывающего обучения, фундаментальности образования и его профессиональной направленности, доступности и строгости изложения теоретического материала, связи теории с практикой, системности и прочности знаний, спиралевидности
Компетенции
Коммуникативность, ответственность, рефлексия, способность к саморазвитию, повышенная профессиональная активность
Программа развития
Информационно-теоретическое (усвоение необходимой информации). Практико-ориентированное (ознакомление с методами деятельности, формирование частных умений). Комплексно-репродуктивное (решение комплексных задач). Проектно-творческое (формирование навыков, опыта практической деятельности)
Мотивационно-целевой компонент
Функции
Мотивационная, целеполагающая
Факторы
Факторы внешней среды: специфика социально-профессиональных отношений, требования работодателей, профессионально-образовательная культура вуза, статус и престиж профессии в обществе
Факторы внутренней среды: социокультурное пространство профессии, ее специфика, индивидуальный профессиональный опыт, специфика отношений со смежными узконаправленными направлениями
Стадии
Формирование первичного, конкретного мотивов
Выбор конкретной цели и побуждение к действию
Результат
Стремление к освоению профессиональной культуры инженера
Методическая система формирования профессиональной культуры студентов инженерных специальностей
Процессуальный компонент
Функции
Трансляционная, презентационная
Методы
Монологичные, диалогичные, проблемные, проектные, игровые, тренинговые, рефлексные, интерактивные, поисковые и т. п.
Формы
Бинарные лекции, лекции-конференции, PR-проекты, деловые и сюжетно-ролевые игры, тренинг, конкурсы, проектные семинары, практикумы, имидж-мастерская внеаудиторные занятия и др.
Этапы развития
Пропедевтический, организационно-прогностический, процессуально-стимулирующий, интеграционно-корректирующий
Контрольно-оценочный компонент
Функции
Диагностическая, корректирующая
Критерии, показатели
Мотивационно-ценностный, когнитивный, деятельностный, коммуникативный, рефлексивный, социокультурный, сформированность профессионально важных качеств личности
Уровни
Адаптивный, репродуктивный, креативный
Инструменты
Кейс-проекты, устные ответы, тестовые задания, контрольные работы, расчетно-графические работы, индивидуальные задания исследовательского или проектного характера
Профессиональная культура инженера сформирована

Таким образом, мы выделяем следующие особенности педагогического сопровождения процесса формирования профессиональной культуры будущих инженеров:

- актуализация потенциальных возможностей образовательного процесса посредством внедрения интерактивных методов обучения, обусловленных требованиями профессиональной деятельности;
- активизация практико-ориентированного проектного обучения, в частности проектно-инженерной деятельности, связанной с функционированием объектов профессиональной деятельности.

Выделенные особенности процесса обучения будущих инженеров позволили нам разработать структуру методической системы формирования профессиональной культуры студентов на основе педагогического сопровождения, которая содержит целевой, содержательный, процессуальный и контрольный компоненты (рис. 1).

В качестве критериев оценки эффективности методической системы формирования профессиональной культуры студентов в системе высшего технического образования выступают мотивационно-ценностный, когнитивный, деятельностный, коммуникативный, рефлексивный, социокультурный критерии, а также критерий сформированности профессионально важных качеств личности.

Для инженера важна не столько энциклопедическая грамотность, сколько способность применять обобщенные знания и умения для разрешения конкретных ситуаций и проблем, возникающих в реальной профессиональной деятельности.

**Заключение**

Таким образом, ведущей целью технического вуза является формирование и развитие у студентов ключевых квалификаций, которые включают коммуникативность, ответственность, рефлексию, способность к саморазвитию, повышенную профессиональную активность, являются одним из этапов процесса формирования профессиональной культуры. Успешная профессиональная деятельность будущего инженера предполагает не только высокий уровень обучения и образования, но и духовно-нравственной, социально-психологической и информационной культуры человека. Выпускник технического вуза должен обладать не только знанием предметной среды профессиональной деятельности, но и высоким уровнем профессиональной культуры как основы его конкурентоспособности в условиях динамики социально-экономических условий в единстве трех ее структурных компонентов: аксиологического, технологического и личностно-творческого.

Опираясь на вышесказанное, нам представляется целесообразным организовывать учебно-воспитательный процесс в техническом вузе, направленный на формирование профессиональной культуры будущих инженеров, в соответствии с разработанной методической системой.

**Литература**

1. Булдык Г.М. Сущность, структура и функции профессиональной культуры инженера // Профессиональное образование, 2021. – № 3. – С. 34-38.
2. Булдык Г.М. Формирование профессиональной культуры инженера // Педагогическая наука и образование, 2021. – № 4. – С. 76-83.

3. Бетуганова М.Б. Формирование профессиональной компетентности будущих инженеров в среде информационных технологий // автореф. дис. канд. пед. Наук, 2006. – 26 с.
4. Фокин Ю.Г. Пути совершенствования методов обучения в высшей школе: Методические рекомендации. – М.: 1991. – С. 4-10.
5. Шагеева Ф. Современные образовательные технологии (опыт инженерного вуза) // Высшее образование в России, 2006. – № 4. – С. 129-132.