УГРОЗЫ КВАНТОВЫХ ВЫЧИСЛЕНИЙ ДЛЯ СУЩЕСТВУЮЩИХ МЕТОДОВ ШИФРОВАНИЯ В ВОЛС

Бекиров Ремзи,
независимый исследователь,
Германия, г. Эссен

E-mail: remzi9082@gmail.com

Аннотация. Развитие квантовых вычислений представляет серьезную угрозу для современных криптографических методов, используемых для защиты данных в волоконно-оптических линиях связи. В статье рассматриваются потенциальные риски, связанные с применением квантовых алгоритмов, таких как алгоритм Шора и алгоритм Гровера, способных значительно снизить стойкость широко используемых криптографических систем, включая RSA, Diffie-Hellman и алгоритмы на основе эллиптических кривых. Анализируется влияние этих технологий на безопасность передачи данных в магистральных и корпоративных оптических сетях. Особое внимание уделяется возможным направлениям повышения криптографической устойчивости, включая постквантовую криптографию и технологии квантового распределения ключей. Рассматриваются перспективы адаптации существующей инфраструктуры ВОЛС к новым требованиям информационной безопасности в условиях развития квантовых вычислительных систем.

Ключевые слова: квантовые вычисления, криптография, безопасность ВОЛС, алгоритм Шора, алгоритм Гровера, постквантовая криптография, квантовое распределение ключей, информационная безопасность, оптические сети, шифрование данных.

Актуальность исследования. Развитие цифровой инфраструктуры и рост объёмов передаваемых данных делают вопросы информационной безопасности ключевыми для функционирования современных телекоммуникационных систем.

Волоконно-оптические линии связи (ВОЛС) являются основой глобальных сетей передачи данных, включая магистральные интернет-каналы, корпоративные сети, банковские системы и государственные информационные ресурсы. Несмотря на высокую пропускную способность и относительную устойчивость оптических каналов к физическим помехам, безопасность передаваемой информации в таких сетях в значительной степени зависит от криптографических методов защиты. В настоящее время широко применяются

алгоритмы шифрования с открытым ключом, такие как RSA, Diffie–Hellman и криптография на основе эллиптических кривых, которые обеспечивают конфиденциальность и аутентификацию при передаче данных.

Однако стремительное развитие квантовых вычислений создает принципиально новые угрозы для существующих криптографических механизмов. Квантовые алгоритмы, в частности алгоритм Шора, способны эффективно решать задачи факторизации больших чисел и вычисления дискретных логарифмов, на сложности которых основана безопасность большинства современных криптосистем. Это означает, что при появлении достаточно мощных квантовых компьютеров значительная часть используемых сегодня методов шифрования может стать уязвимой. В контексте ВОЛС это представляет особую проблему, поскольку такие сети используются для передачи важной информации на большие расстояния и в больших объёмах.

Дополнительную актуальность исследованию придаёт концепция «перехватить сейчас – расшифровать позже», при которой злоумышленники могут сохранять зашифрованные данные с целью их последующей расшифровки при появлении квантовых вычислительных средств. В связи с этим возникает необходимость анализа потенциальных угроз квантовых вычислений для существующих методов шифрования, применяемых в оптических сетях, а также поиска перспективных решений, способных обеспечить криптографическую устойчивость ВОЛС в условиях развития квантовых технологий. К таким решениям относятся методы постквантовой криптографии и системы квантового распределения ключей, которые рассматриваются как возможные направления модернизации систем защиты информации.

Цель исследования. Целью данного исследования является анализ угроз, возникающих в результате развития квантовых вычислений для существующих методов криптографической защиты данных, применяемых в волоконно-оптических линиях связи, а также оценка возможных направлений повышения устойчивости систем шифрования в оптических сетях.

Исследование направлено на выявление уязвимостей традиционных криптографических алгоритмов в условиях использования квантовых вычислительных технологий, изучение принципов работы квантовых алгоритмов, влияющих на криптографическую стойкость, а также рассмотрение перспектив внедрения постквантовых криптографических решений и квантовых технологий защиты информации.

Достижение поставленной цели предполагает комплексный анализ современных криптографических методов, применяемых в телекоммуникационных системах, и оценку их устойчивости к потенциальным атакам с использованием квантовых вычислений.

Материалы и методы исследования. В рамках исследования использованы теоретические и аналитические методы изучения проблемы безопасности криптографических систем в волоконно-оптических сетях в условиях развития квантовых вычислений.

Материалами исследования послужили научные публикации в области квантовых вычислений, криптографии и телекоммуникационных технологий,

международные стандарты информационной безопасности, а также результаты современных исследований, посвящённых постквантовой криптографии и квантовому распределению ключей.

Были проанализированы принципы функционирования классических криптографических алгоритмов, используемых в системах защиты данных, передаваемых по ВОЛС, включая RSA, Diffie-Hellman и алгоритмы на основе эллиптических кривых.

Методологическую основу исследования составили методы сравнительного анализа, системного анализа и теоретического моделирования. Сравнительный анализ позволило поставить устойчивость традиционных криптографических алгоритмов с потенциальными возможностями квантовых алгоритмов, таких как алгоритм Шора и алгоритм Гровера.

Системный подход применялся для оценки влияния квантовых вычислений на комплексную архитектуру безопасности оптических сетей и выявления уязвимых элементов в существующих схемах защиты информации. Также использовались методы обобщения и интерпретации результатов научных исследований, направленных на разработку новых криптографических подходов, устойчивых к квантовым атакам.

В ходе исследования также рассматривались перспективные направления повышения безопасности ВОЛС, включая внедрение постквантовых криптографических алгоритмов, основанных на решении задач теории решёток, кодовой криптографии и хэш-функций, а также использование технологий квантового распределения ключей, обеспечивающих высокий уровень защиты каналов связи благодаря фундаментальным законам квантовой физики.

Применение данных методов анализа позволило сформировать комплексное представление о потенциальных рисках для существующих систем шифрования и определить возможные пути адаптации телекоммуникационной инфраструктуры к новым условиям развития квантовых вычислительных технологий.

Результаты исследования. Развитие методов шифрования в волоконно-оптических линиях связи тесно связано с эволюцией телекоммуникационных сетей и криптографических технологий.

Первые оптические линии связи начали активно внедряться в 1970-е годы, когда стало очевидно, что передача данных по оптоволокну обладает значительно большей пропускной способностью и устойчивостью к электромагнитным помехам по сравнению с медными линиями. Однако на ранних этапах основное внимание уделялось физическим характеристикам канала связи, таким как скорость передачи, затухание сигнала и надежность оборудования. Вопросы криптографической защиты в тот период рассматривались отдельно от самой линии связи и реализовывались преимущественно на уровне конечных устройств или сетевых протоколов.

В 1980-е годы с развитием цифровых сетей передачи данных начали широко применяться симметричные алгоритмы шифрования. Одним из наиболее распространённых стал алгоритм DES (Data Encryption Standard), который

использовался для защиты каналов связи в телекоммуникационных системах и корпоративных сетях [6]. В ВОЛС шифрование обычно выполнялось на уровне сетевого оборудования, например в мультиплексорах и маршрутизаторах. Хотя оптоволоконный кабель сложнее перехватить по сравнению с традиционными проводными линиями, угрозы несанкционированного доступа всё же существовали, что требовало применения криптографических механизмов защиты.

В 1990-е годы, с быстрым развитием интернета и глобальных сетей передачи данных, требования к безопасности значительно возросли. В этот период активно внедрялись алгоритмы шифрования с открытым ключом, такие как RSA и протокол обмена ключами Диффи-Хеллмана [4]. Они позволили безопасно распределять криптографические ключи между удалёнными узлами сети, что стало важным этапом развития защищённых коммуникаций в оптических сетях. Одновременно с этим начали применяться более устойчивые симметричные алгоритмы, включая Triple DES.

В конце 1990-х и начале 2000-х годов был принят новый стандарт симметричного шифрования AES (Advanced Encryption Standard), который стал основой для защиты данных в большинстве современных сетей, включая системы передачи по ВОЛС. AES обеспечивал высокую криптографическую стойкость и эффективность обработки данных, что было особенно важно для высокоскоростных оптических каналов. В этот период также получили широкое распространение защищённые сетевые протоколы, такие как IPsec, SSL и TLS, которые обеспечивали шифрование данных на уровне сетевых соединений [1].

С увеличением пропускной способности оптических сетей и переходом к технологиям DWDM (Dense Wavelength Division Multiplexing) возникла необходимость в специализированных системах шифрования, способных работать на скоростях десятков и сотен гигабит в секунду. Это привело к развитию аппаратных систем шифрования, интегрированных непосредственно в оптическое сетевое оборудование. Такие решения обеспечивали так называемое канальное шифрование, при котором данные защищаются непосредственно в транспортной сети, а не только на уровне приложений.

К середине 2000-х годов многие производители телекоммуникационного оборудования начали внедрять встроенные криптографические модули в оптические транспондеры, мультиплексоры и маршрутизаторы. Это позволило реализовать высокоскоростное шифрование трафика без существенного снижения производительности сети. Наиболее часто применялись алгоритмы AES с длиной ключа 128 или 256 бит, которые обеспечивали высокий уровень безопасности при передаче данных по магистральным ВОЛС [3].

В последние годы значительное внимание уделяется угрозам, связанным с развитием квантовых вычислений. Классические криптографические алгоритмы с открытым ключом, широко используемые для обмена ключами и аутентификации в оптических сетях, могут стать уязвимыми при появлении мощных квантовых компьютеров. Это стимулировало развитие новых направлений защиты информации (рис. 1).

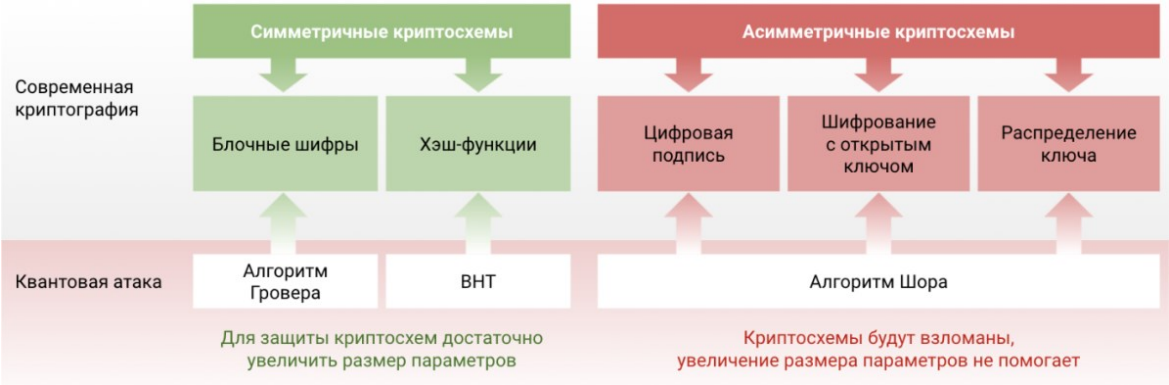

Рис. 1 Постквантовая криптография

Одним из таких направлений стало квантовое распределение ключей (Quantum Key Distribution, QKD). Эта технология использует свойства квантовой физики для безопасной передачи криптографических ключей по оптоволоконным каналам. В отличие от классических методов шифрования, безопасность QKD основана на фундаментальных физических законах, что делает невозможным незаметный перехват ключа [2]. Первые экспериментальные системы квантового распределения ключей начали разрабатываться в 1990-е годы, а в настоящее время они активно тестируются и внедряются в магистральных оптических сетях.

Параллельно развивается направление постквантовой криптографии, целью которого является создание алгоритмов шифрования, устойчивых к атакам квантовых компьютеров. Такие алгоритмы основаны на математических задачах, которые остаются сложными даже для квантовых вычислений, например на задачах теории решёток или кодовой криптографии.

На современном этапе методы шифрования в ВОЛС представляют собой комплексную систему защиты, включающую несколько уровней безопасности. Шифрование может осуществляться на уровне приложений, сетевых протоколов, транспортного уровня и непосредственно на уровне оптического канала (табл. 1). Современные системы передачи данных используют сочетание симметричных алгоритмов высокой производительности и асимметричных механизмов распределения ключей.

Развитие технологий оптической связи, увеличение скорости передачи данных до сотен гигабит и терабит в секунду, а также появление новых вычислительных угроз требуют постоянного совершенствования криптографических методов. В связи с этим современные исследования направлены на интеграцию постквантовых алгоритмов и квантовых технологий защиты в инфраструктуру волоконно-оптических сетей, что должно обеспечить долгосрочную безопасность глобальных систем передачи информации.

Отметим, что волоконно-оптические линии связи широко используются для передачи больших объёмов информации в телекоммуникационных сетях, центрах обработки данных, банковских системах и государственных инфраструктурах.

Таблица 1

Основные методы шифрования в ВОЛС

№	Метод	Характеристика
1	Симметричное шифрование	Использует один и тот же ключ как для шифрования, так и для расшифровки. Примеры: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
2	Асимметричное шифрование	Использует пару ключей: открытый и закрытый. Примеры: RSA, ECC (Elliptic Curve Cryptography).
3	Шифрование на уровне канала	Шифрование происходит на уровне транспортного или канального протокола, например, с использованием IPSec для защиты IP-трафика.
4	Шифрование на уровне приложения	Данные шифруются непосредственно в приложениях перед передачей по ВОЛС. Это позволяет защитить данные независимо от используемой технологии передачи.
5	Криптографические протоколы	Использование протоколов, таких как TLS (Transport Layer Security), для защиты данных при их передаче по сети.
6	Масштабируемые методы	Использование распределенного шифрования, где данные разбиваются на
7	Квантовое шифрование	Использует принципы квантовой механики для обеспечения безопасно-

Несмотря на высокую физическую защищённость оптоволоконных каналов, безопасность передаваемых данных в основном обеспечивается криптографическими методами. Большинство современных систем защиты в ВОЛС основаны на классических криптографических алгоритмах, которые предполагают ограниченные вычислительные возможности потенциального злоумышленника. Появление квантовых вычислений создаёт серьёзные угрозы для таких методов шифрования, поскольку квантовые алгоритмы способны значительно ускорять решение некоторых математических задач, лежащих в основе современной криптографии.

Переход к квантово-безопасным волоконно-оптическим сетям потребует от операторов связи глубокой трансформации бизнеса, что неизбежно повлечет за собой серьезные финансово-экономические последствия. Операторам придется столкнуться с существенным ростом как капитальных, так и операционных расходов из-за необходимости масштабных инвестиций в закупку нового оборудования, поддерживающего алгоритмы постквантовой криптографии, и аппаратуры квантового распределения ключей.

Эксплуатация таких систем потребует больше энергии и более квалифицированного обслуживания. Кроме того, существующие шлюзы безопасности и маршрутизаторы, не обладающие аппаратным ускорением для новых алгоритмов, морально устареют быстрее своих нормативных сроков службы, что приведет к ускоренной амортизации. К этому добавятся значительные затраты на проведение глобальной криптографической инвентаризации всей сетевой инфраструктуры для выявления уязвимых узлов и оценки объемов трафика, требующего приоритетной защиты.

Эти финансовые вложения напрямую продиктованы технико-архитектурными изменениями, которые затронут как оптический, так и IP-уровни сетей. Внедрение алгоритмов постквантовой криптографии многократно увеличит размер криптографических ключей и служебных заголовков, что потребует обновления процессоров в коммутационном оборудовании для предотвращения падения пропускной способности и роста задержек в магистральных каналах.

Если же оператор сделает ставку на физическую защиту через квантовое распределение ключей, ему придется решать сложнейшие инженерные задачи по планированию сетей спектрального уплотнения. Это потребует либо выделения отдельных «темных» волокон, либо внедрения дорогостоящей спектральной фильтрации для совместной передачи квантовых и классических сигналов, что неизбежно ограничит максимальную дальность и мощность основного оптического трафика. В результате операторам придется переходить к гибридным архитектурам, где классическая криптография, постквантовые алгоритмы и квантовое распределение ключей будут работать в связке, требуя разработки совершенно новых протоколов управления сетью.

Реализация этих архитектурных сдвигов породит серьезные операционно-управленческие вызовы, связанные в первую очередь с острым дефицитом кадров. Инженерам по сетевой безопасности и оптикам потребуется освоить новые компетенции на стыке квантовой физики и сложной математики, что потребует масштабных программ переобучения. Операторам также предстоит выстроить беспрецедентно сложный процесс управления жизненным циклом и миграции, обеспечив бесшовный переход на новые стандарты без прерывания обслуживания, что потребует внедрения продвинутых систем оркестрации, способных динамически переключать профили шифрования.

Параллельно с этим перед ними встанет задача борьбы с атаками по принципу «собрать сейчас, расшифровать позже», вынуждая срочно внедрять механизмы ретроактивной защиты для трафика с длительным сроком жизни, чтобы предотвратить будущую компрометацию архивных данных, перехваченных злоумышленниками сегодня.

В конечном итоге все эти трансформации кардинально скажутся на стратегическом и коммерческом позиционировании операторов на рынке. С одной стороны, квантово-безопасные каналы связи станут новым премиальным продуктом с высокой добавленной стоимостью, позволяя продавать защищенные виртуальные сети и выделенные линии банкам, госкорпорациям и медицинским учреждениям. С другой стороны, операторы столкнутся с нарастающим регуляторным давлением и необходимостью строгого комплаенса по мере выпуска национальными регуляторами обязательных стандартов постквантового перехода, где несоблюдение сроков миграции грозит штрафами и потерей лицензий на обслуживание критической инфраструктуры. Дополнительно им придется пересмотреть отношения с вендорами телеком-оборудования, сделав важным требование к поставщикам предоставлять квантово-безопасные обновления и гарантировать отсутствие скрытых уязвимостей в новых

криптографических чипах, превращая квантовую защиту из вынужденной статьи расходов в мощный инструмент стратегического позиционирования и монетизации.

По мнению автора, текущий уровень готовности современной телекоммуникационной инфраструктуры, и в частности магистральных волоконно-оптических линий связи, к постквантовому переходу как низкий, характеризующийся уязвимостью и отсутствием унифицированных механизмов защиты.

Фундаментальная проблема заключается в том, что глобальная сетевая архитектура исторически построена на классических асимметричных алгоритмах, таких как RSA и ECC, которые математически беззащитны перед лицом зрелых квантовых компьютеров. Несмотря на растущее осознание угрозы атак по принципу «собрать сейчас, расшифровать позже», реальная готовность аппаратно-программной базы остается минимальной. Большинство эксплуатируемых сегодня оптических транспортных систем, маршрутизаторов и шлюзов безопасности не обладают необходимой вычислительной мощностью и объемом памяти для обработки постквантовых алгоритмов.

Внедрение алгоритмов PQC требует использования криптографических ключей колоссального размера и значительных вычислительных ресурсов, что при интеграции в существующие терабитные оптические каналы неизбежно ведет к падению пропускной способности и росту задержек, что неприемлемо для современных сетей передачи данных.

Ситуация усугубляется тем, что альтернативные методы физической защиты, такие как системы квантового распределения ключей (QKD), также находятся на крайне ранней стадии коммерческой зрелости для массового телекома. Зачастую QKD ошибочно воспринимается как готовое «серебряное пуле», однако на практике его интеграция в плотные спектральные сети (DWDM) сталкивается с серьезнейшими инженерными барьерами. Квантовые каналы страдают от жестких ограничений по дальности передачи, требуют прокладки выделенных «темных» волокон или сложнейшей и дорогостоящей спектральной фильтрации для совместной работы с классическими оптическими сигналами высокой мощности.

В результате отрасль фактически лишена единого, масштабируемого и экономически целесообразного технологического стека, способного обеспечить квантово-безопасную передачу данных в оптическом диапазоне без радикальной перестройки физической инфраструктуры. Стандарты постквантовой криптографии, разрабатываемые международными институтами, пока не трансформировались в готовые отраслевые спецификации для телекоммуникационного оборудования, что оставляет операторов в состоянии неопределенности относительно выбора долгосрочной архитектуры защиты.

Резюмируя, автор считает, что современная телекоммуникационная инфраструктура находится в кризисном состоянии и фундаментально не готова к безболезненному постквантовому переходу. Преодоление этого разрыва потребует не просто программных обновлений, а беспрецедент по масштабу и

стоимости цикл аппаратной модернизации, включающий замену кремниевой базы в DSP-процессорах оптических трансиверов, внедрение принципов криптографической гибкости (crypto-agility) на всех уровнях сетевой модели и пересмотр самих принципов построения магистральных каналов.

Игнорирование этой проблемы или попытка отложить миграцию до момента появления полноценных квантовых компьютеров станет ошибкой, поскольку инерция обновления глобальной оптической инфраструктуры исчисляется десятилетиями, а окно для упреждающей защиты данных с длительным сроком конфиденциальности стремительно закрывается уже сегодня.

Заключение. Таким образом, по мнению автора, квантовые вычисления представляют не отдаленную теоретическую, а уже актуальную стратегическую угрозу для существующих методов шифрования в волоконно-оптических линиях связи.

Развитие квантовых алгоритмов, таких как алгоритм Шора, делает принципиально уязвимыми широко используемые асимметричные криптосистемы (RSA, ECC), на которых базируется безопасность современных оптических сетей и протоколов обмена ключами.

Особую опасность в текущих реалиях представляет тактика «собрать сейчас, расшифровать позже» (Harvest Now, Decrypt Later), при которой злоумышленники уже сегодня перехватывают и архивируют зашифрованный трафик, передаваемый по магистральным ВОЛС, ожидая появления достаточно мощных квантовых компьютеров для его ретроспективного взлома. Это означает, что конфиденциальные данные с длительным сроком жизни (государственные секреты, интеллектуальная собственность, биометрические данные) находятся под прямой угрозой уже в настоящий момент, что диктует необходимость немедленного начала миграции на квантово-устойчивые решения, не дожидаясь появления полноценного универсального квантового компьютера.

Автор считает, что переход к квантово-безопасным ВОЛС сопряжен с серьезными инженерно-техническими и экономическими вызовами, требующими комплексной перестройки сетевой архитектуры. Внедрение алгоритмов постквантовой криптографии (PQC) в оптические транспортные сети неизбежно ведет к увеличению вычислительной нагрузки на DSP-процессоры и сетевое оборудование, что может повлиять на задержки и общую пропускную способность высокоскоростных терабитных каналов.

В то же время, использование квантового распределения ключей (QKD), хотя и обеспечивает безусловную физическую безопасность, сталкивается с фундаментальными ограничениями: потерями фотонов на больших расстояниях, высокой стоимостью развертывания выделенных волокон или сложных спектральных фильтров в системах DWDM, а также уязвимостью самих фотонных детекторов к атакам по сторонним каналам. Таким образом, изолированное применение только одного из этих подходов не способно обеспечить надежную, масштабируемую и экономически целесообразную защиту магистральных оптических сетей.

Наиболее перспективным направлением является разработка и внедрение гибридных криптосистем, органично сочетающих математическую стойкость алгоритмов постквантовой криптографии с физической защищенностью квантового распределения ключей на базе фотонных интегральных схем (PIC). Интеграция миниатюрных QKD-модулей непосредственно в кремниевые фотонные чипы оптических трансиверов позволит радикально снизить габариты, стоимость и энергопотребление оборудования, а также упростить его масштабирование в существующих оптических сетях без необходимости прокладки выделенных линий связи.

Параллельно с этим важным шагом является ускоренная отраслевая стандартизация таких гибридных решений (в рамках ITU-T, ETSI и IETF) и проведение сквозной криптографической инвентаризации сетевого оборудования для плавной, поэтапной миграции. Именно такой симбиоз алгоритмической и физической защиты оптического уровня сформирует новый, неуязвимый стандарт безопасности глобальных телекоммуникационных инфраструктур в постквантовую эпоху.

Литература:

1. Бабин В. С. Современные тенденции развития систем специальной связи и показателей эффективности процесса их функционирования // Сборник статей Международной научно-практической конференции, «Молодёжная наука», Пенза МЦНС «Наука и Просвещение» 2020 30.10.2020 г. Пенза. – 2020. – С. 37-40.

2. Жиляев А.Е. Сети квантового распределения ключей в кибербезопасности. Научное издание. М: Горячая линия – Телеком, 2022. – 152 с.

3. Коновалов А.С. Особенности построения системы специальной связи на базе волоконно-оптических линий // Инженерный вестник Дона. – №5 (101). – 2021. – С. 69-76.

4. Khorov E. et al. A tutorial on IEEE 802.11 ax high efficiency WLANs // IEEE Communications Surveys & Tutorials. – 2018. – Т. 21. – № 1. – С. 197-216.

5. Moody D. Nist pqc standardization update //National Institute of Standards and Technology. – 2021. – С. 2021-10.

6. Sang Z., Li K. ITU-T standardisation activities on smart sustainable cities // IET smart cities. – 2019. – Т. 1. – № 1. – С. 3-9.