ЭКОНОМИКА

УДК 004.65

DOI: 10.21779/2500-1930-2025-40-3-7–19

Ю. А. Капустина[1], Г. В. Федотова[2]

Кибербезопасность информационной инфраструктуры в условиях квантового превосходства

[1] Уральский государственный лесотехнический университет; Россия, 620100, Екатеринбург, Сибирский тракт, 37; kapustina_bu@mail.ru;

[2] Федеральный исследовательский центр «Информатика и управление» РАН; Россия, 119333, Москва, ул. Вавилова, 44, корп. 2; g_evgeeva@mail.ru

Аннотация. Усиление геополитических противостояний в мировом пространстве и нарастание технологического превосходства одних стран над другими ставят под угрозу российскую информационную инфраструктуру, которая постоянно подвергается атакам кибермошенников с нелегального Интернет-пространства. Растет количество и расширяется разнообразие кибератак, в связи с чем подвергается постоянному тестированию на устойчивость система информационной безопасности. Высокая импортозависимость российского цифрового пространства стала причиной уязвимости российской цифровой инфраструктуры после ухода в 2022 году иностранных поставщиков программного обеспечения и технологий. Активность мошенников растет, появляются новые виды вредоносных программ, поэтому необходимо стимулировать поиск и увеличить финансирование принципиально иных технологических решений для противостояния внешнему вмешательству в информационное пространство.

Квантовые исследования, которыми занимаются сегодня передовые технологические корпорации, национальные юрисдикции – это новая ступень развития общественной цифровизации. Возможности, которые открывает перед миром вторая квантовая революция, дискредитируют криптографические подходы к шифрованию и защите инфраструктуры, но дают новые инструменты для продвижения информационной инфраструктуры и ее совершенствования. Авторами сделаны выводы о необходимости оперативной интеграции квантовых достижений в уже существующие системы поддержания устойчивости и безопасности цифровой среды.

Ключевые слова: информационная инфраструктура, цифровая среда, безопасность, мошенники, хакеры, кибербезопасность, устойчивость, защита цифрового периметра, вредоносные программы, данные.

Введение

Глобальный переход в онлайн-среду и погружение в виртуальную реальность способствуют появлению не только новых направлений развития экономики услуг, но и новых рисков, связанных с данными. Основными ценными активами информационной инфраструктуры являются данные, т. е. цифровые ресурсы различного свойства (персональные данные, имущественные права, цифровые финансовые активы, электронные документы, пароли и коды). Все эти информационные ресурсы, попадая в DarkNet, формируют новую цифровую реальность теневой экономики – экономику хактивизма, в которой данные становятся реальным товаром и приносят доходы своим продавцам.

Кибермошенники все чаще атакуют информационную среду, похищая данные, которые могут быть использованы в нелегальных целях и дискредитировать их владельцев. По этой причине необходимо четко идентифицировать риски потери данных, укреплять собственную цифровую защиту и правильно реагировать на их утрату.

Последние 10 лет статистика кибератак демонстрирует неуклонный рост количества инцидентов с системами безопасности критической информационной инфраструктуры России. По итогам 2024 года количество атак выросло на 20 %, экономический ущерб от них составил 200 млрд руб. Эти цифры больше показателей 2023 года на 30 %, и по прогнозам следующие 3–4 года они продолжат расти. Рассмотрим, какими методами пользуются хакеры при совершении атак на информационную инфраструктуру [1] (рис. 1).

Максимальное количество атак производится с целью заражения цифровых систем вредоносными программами (29 %), на втором месте – срабатывание сигнатуры сенсоров SOL (12 %), на третьем – сетевые атаки (10 %). Выведение из эксплуатации, нарушение работоспособности и устойчивости информационной инфраструктуры – основные цели деятельности хакеров.



Рис. 1. Структура и характер кибератак на российскую информационную инфраструктуру в 2024 году, %

Источник: составлено по [1].

Больше всего было атак с заражением вредоносными ПО, которые обнаруживались постфактум, что фактически исключало возможность их удаления. К моменту обнаружения такого объекта он уже успевал запустить процесс дезорганизации или нанести вред среде. В таком случае необходимо привлекать дополнительные ресурсы для купирования программы-вируса и настройки работы среды [2; 3].

Устранение последствий хакерских атак требует времени, и это дает возможность мошенникам спланировать новую атаку и даже написать программу с учетом специфики защиты и работы конкретной информационной среды [4]. Для этих целей злоумышленники достаточно активно используют в своих разработках новые техноло-

гии. Поэтому необходимо задействовать технологии AI, машинного обучения и вести поиск в направлении применения квантовых технологий.

Фактически киберпространство становится вторым онлайн-фронтом, где каждую секунду происходят атаки и их нейтрализация средствами информационной защиты. Специалисты многих государств ведут поиск в направлении квантовых вычислений и коммуникаций, сенсорики и метрологии для достижения квантового превосходства и создания защищенной информационной среды.

Методы и материалы

Проведенное научное исследование базировалось на основополагающих общенаучных методах познания:

– посредством аналитического метода были изучены современные процессы трансформации привычных бизнес-процессов и явлений, происходящие в социально-экономической сфере под влиянием технологического развития;

– с помощью метода синтеза были сформированы однородные совокупности и выделены общие черты и риски цифровизации в мировом информационном пространстве, определены основные тенденции движения современных бизнес-моделей;

– с использованием методов абстрагирования и обобщения были выделены тренды современного информационного развития и определены основные угрозы для устойчивой работы цифровых систем;

– при помощи методов индукции и дедукции были изучены ретроспективные накопленные цифровые данные и сделаны выводы о прогнозном росте показателей в будущих периодах.

Исследование практической составляющей было основано на статистическом анализе современных трендов и выстраивания графиков движения изучаемой совокупности.

Теоретической базой научного исследования послужили труды российских и иностранных экономистов, посвященные проблемам цифровизации и кибербезопасности. Особо следует выделить следующих ученых, занимавшихся вопросами поддержания экономической безопасности цифровых систем и сервисов: Р. Р. Ахметов, Г. С. Бударный, В. А. Плотников, А. В. Плотников, С. И. Штеренберг, И. В. Чумаков и др.

Проблемам кибербезопасности и устойчивости критической информационной инфраструктуры уделяли внимание следующие авторы Е. В. Анянова, Ю. А. Баландин, А. А. Бердюгин, А. И. Горев, Е. Г. Горева, Карпенко И. Н., Капустина Ю. А., Ревенков П. В., Федотова Г. В., Францев В. В., Чебарь А. Г.

Усилению криптографических инструментов защиты данных в Интернете посвящены труды российских и иностранных экономистов: Ария К., Вабуш Р., Беликовой К. М., Экерт А. К., Чен Ю. А., Чен Т. Ю., Моска М., Занг К., Юлин Ву.

Источниками эмпирических и цифровых материалов послужили открытые отчеты аналитических компаний, размещенные в интернете, а также нормативно-правовые акты, утвержденные в исследуемой сфере.

Результаты

Колоссальные массивы данных, накопленные в национальной информационной инфраструктуре, представляют собой привлекательную цель для атаки мошенников и хакеров из недружественных России стран. Рост количества попыток дестабилизации работы российской критической информационной инфраструктуры происходит на протяжении последних 14 лет. При этом, по средней статистической оценке, в мире по-

следние 2 года ежегодно формируется 328,77 млн терабайт данных, то есть их число растет экспоненциально. Рассмотрим статистику с 2002 по 2024 гг. включительно. Так, в 2024 году было создано, по мировым оценкам цифровой исследовательской платформы Statista, почти 147 зеттабайт данных. Прогноз на 2025 год положительный и составляет 181 зеттабайт. Динамика роста объемов накопления данных представлена на рисунке 2.

Представленный график на рисунке 2 демонстрирует тенденцию роста объемов созданных цифровых активов в глобальном информационном пространстве. Данными активами следует управлять грамотно и корректно, а также беречь их от краж, утечек, уничтожения и применения в преступных целях [5–7].

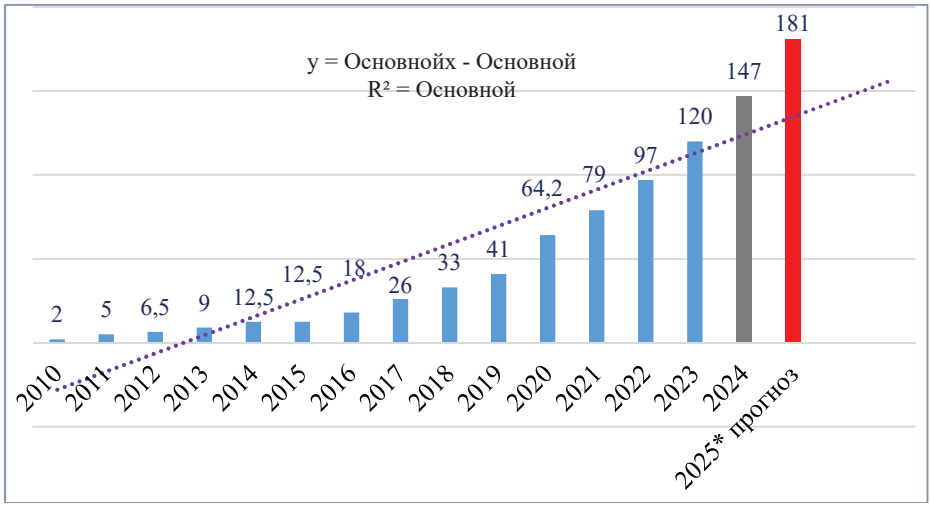


Рис. 2. Количество созданных данных в мировой цифровой среде, зеттабайт

Источник: составлено по [3].

Помимо темпов накопления данных в глобальном интернет-пространстве растет стоимость цифрового ресурса. Так, в 2024 году стоимость рынка Больших данных оценивалась экспертами на сумму 349,56 млрд долл. Рассмотрим темпы роста и прогнозные показатели объема сектора данных (рис. 3).

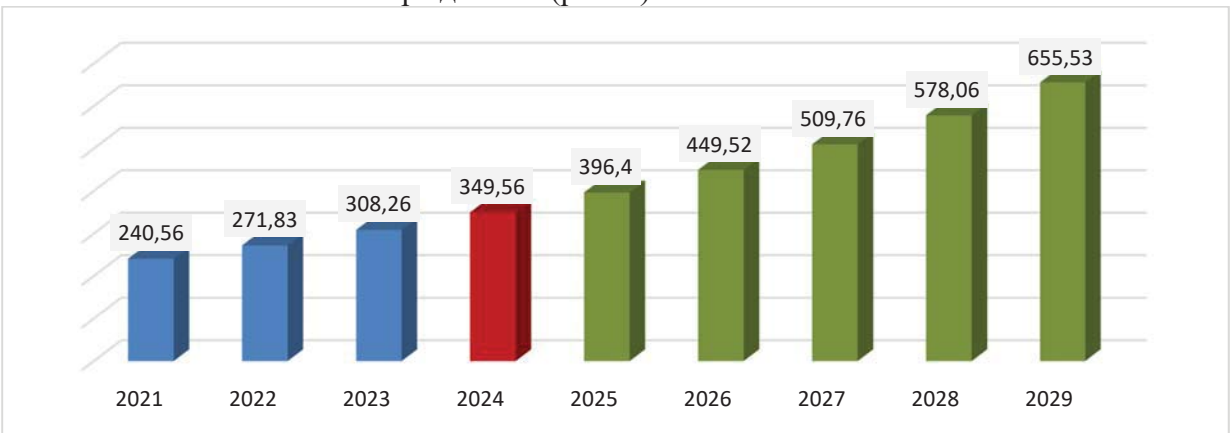


Рис. 3. Стоимость международного рынка Больших Данных, млрд долл.

Источник: составлено по [8].

Представленная динамика мирового рынка данных свидетельствует, что в среднем он растет на 13 % в год на протяжении 5 лет, при этом темпы не падают, и к 2029 году его масштабы достигнут 655,53 млрд долл. Такие цифры достаточно внушительны, поэтому рынок данных все чаще подвергается атаками кибермошенников.

Дистанционное обслуживание клиентов, удаленные рабочие места, онлайн-регистрация на мероприятия, общение в социальных сетях, удаленное оформление услуг и товаров – все это наша современная реальность, которая генерирует риски потери данных в киберсреде [9; 10]. Данные риски имеют тенденцию к росту по мере усложнения и масштабирования рабочего и досугового пребывания пользователей в информационном пространстве [11].

Современная статистика свидетельствует, что 80 % домашних роутеров являются уязвимыми. 90 % вирусов проникает в ПК через вложения электронных писем, 96 % кибератак обнаруживается через месяц после взлома. По итогам 2024 года общее количество кибератак на информационную инфраструктуру России выросло на 630 % в сравнении с 2023 годом (согласно отчетам компании «Информзащита»). Представленные цифры достаточно серьезны. Необходимо тщательно их анализировать и искать новые превентивные меры противодействия подобным угрозам [12; 13].

Работа по защите информационной инфраструктуры ведется постоянно на всех уровнях: выстроена государственная система защиты информационного пространства ГосСОПКА, на предприятиях установлены программы защиты данных, проводится политика импортозамещения, и все операционные действия переводятся на ПО российского производства [14; 15]. Рассмотрим особенности некоторых мер.

Согласно ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), которая фактически представляет собой электронную платформу, аккумулирующую информацию об инцидентах на объектах критической информационной инфраструктуры, перечень которых также определен законодателем [16]. Фактически это государственный цифровой контроль информационной безопасности в наиболее социально-экономически важных для государства сферах общественной жизни и отраслях народного хозяйства.

На уровне рыночных субъектов и учреждений государственного сектора функционируют системы цифровой безопасности, интегрированные в структуру ГосСОПКА и формирующие своеобразную модель государственно-частного партнерства в данной сфере. Угрозы кибербезопасности актуальны для всех информационных систем, поэтому по данному вопросу появляются коллаборативные объединения [17; 18].

Выстраивание самостоятельной системы защиты от таких атак – достаточно ресурсоемкий процесс. Могут возникать риски по мере интеграции автономной системы в национальное информационное пространство [19]. По данной причине нужен единый координирующий центр, который будет цифровым щитом поддерживать все включенные в систему инфраструктурные объекты. ГосСОПКА фактически выступает центром по аккумулированию всей информации об атаках на российскую критическую инфраструктуру, который оперативно обрабатывает и выстраивает новые алгоритмы защиты от хакерских атак.

Бизнес может самостоятельно включаться в ГосСОПКУ и тем самым обеспечить себе гарантии цифровой безопасности и осуществления надзора на уровне государства. Формируется модель партнерства бизнеса и государства, которая представляет собой новую практику выстраивания информационной защиты: взаимодействие государства

и частных структур по коллективному реагированию на инциденты цифровой безопасности. Единая система национальной информационной защиты позволит эффективно функционировать объектам инфраструктуры внутри цифрового пространства, но в любом случае будут появляться риски из внешней среды [20].

Дополнительным фактором повышения устойчивости российской критической информационной инфраструктуры выступает национальный курс на импортозамещение. Согласно Указу Президента РФ № 166 для поддержания технологического суверенитета страны была предписана миграция критической информационной инфраструктуры на российское ПО. Но даже в 2025 году данная работа не будет завершена, что порождает дополнительные риски отказа в обслуживании [1].

Очевидно, что условия переходного периода провоцируют новые риски в киберсреде. Достаточно критичным направлением технологических разработок выступает квантовый поиск, в который включились мировые технологические лидеры. Квантовые вычисления, квантовые коммуникации и сети, квантовая криптография – все это уже будущая реальность, которая выведет общество в новую систему взаимодействия в эпоху квантовых технологий [21; 22].

Квантовый компьютер имеет супервозможности, и это доказано многочисленными исследовательскими командами различных стран. Это и мгновенный взлом сложных криптографических шрифтов, и обход цифровых подписей, и высокоскоростная расчетная производительность, в миллион раз превышающая скорость кремниевых компьютеров. По этой причине в ожидании новой квантовой революции приходится сомневаться в надежности традиционных алгоритмов передачи данных, шифрования, защиты [23; 24].

Мировой рынок квантовых вычислений по итогам 2024 года достиг максимального значения по объемам инвестирования по сравнению с другими IT-сферами и составил 1 млрд долл. США. При этом средний рост объемов затрат на данное направление в среднем растет из года в год на 25 %. Рассмотрим тенденции развития рынка квантовых вычислений (рис. 4).

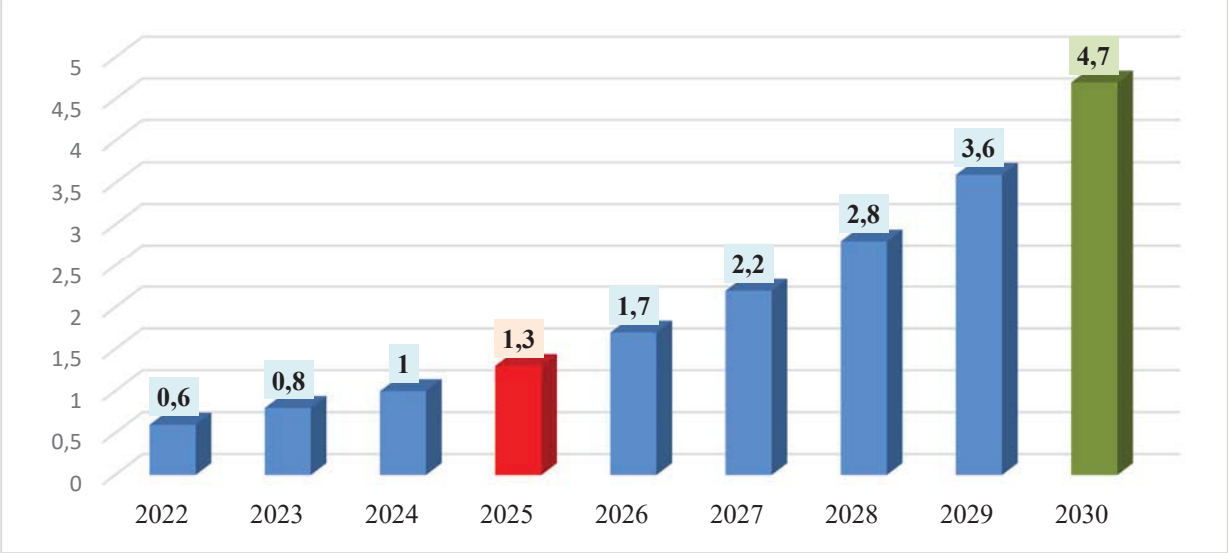


Рис. 4. Инвестиции в мировой рынок квантовых вычислений, млрд долл.

Источник: составлено по [25].

Многие крупные корпорации вкладывают в разработку квантовых технологий колоссальные инвестиции, отчетливо осознавая, перспективы могут открыться перед их разработчиками от моделирования бизнес-процессов до прогнозирования развития рынков. Квантовые компьютеры, которые имеются на сегодняшний день, до сих пор не работают в цифровой среде, и многочисленные исследовательские команды в различных странах занимаются дальнейшим усовершенствованием данных технологий и поиском их практического применения.

Квантовые вычисления достаточно критичны, т. к. их скорость в миллионы раз превышает скорость вычисления на кремниевых компьютерах. Поэтому уже сегодня многие страны работают на опережение, исследуя существующие технологии и пытаясь создать квантовый компьютер, устойчивый к внешним шумам и влияниям. Пока создать квантовый компьютер не удалось, но, по оценкам специалистов, при существующем темпе роста инвестиций в квантовые разработки эта цель может быть достигнута к 2030 году.

Используемые сегодня алгоритмы криптографического шифрования принято считать достаточно надежными при данном уровне развития технологий. Но с помощью квантовых вычислений можно получить доступ к любой существующей конфиденциальной информации. Поэтому многие государства и крупные корпорации стремятся работать на опережение и внедрять некоторые алгоритмы квантовой криптографии, чтобы уже сегодня шифровать данные так, чтобы было невозможно их взломать даже с применением квантовых компьютеров.

Квантовая криптография представляет собой ключи шифрования, основанные на физических свойствах фотонов (изменение фотонов приводит к их изменению в будущем). По данной причине попытки взломов квантовых каналов будут приводить только к информированию владельцев ключей, что практически делает такой шифр киберустойчивым [21].

Подобные алгоритмы уже применяются в различных странах (США, Китай, Канада, ЕС, Россия). Мировые технологические державы разрабатывают новые коммуникационные сети, протоколы, алгоритмы с применением квантовых технологий [22]. Определенные результаты получены как в мировой практике, так и российскими исследовательскими командами.

Так, в России в 2021 году была запущена магистральная квантовая сеть, протяженность которой к 2030 году составит 15 тыс. км. Эффект, который запланирован от запуска данной сети, – расширение радиуса действий квантовых каналов связи и рост скорости передачи данных [25].

В 2024 году были проведены испытания компаниями ИнфоТеКС и ТрансТелеК, которые доказали возможность работы системы квантового распределения ключей в типичных телекоммуникационных сетях с использованием технологии частотного уплотнения каналов. Благодаря этим испытаниям были созданы гибридные технологические системы, устойчивые к киберрискам.

Достижением российских разработчиков является создание 50-кубитного квантового компьютера на ионной платформе с запуском вычислений посредством облачной инфраструктуры. Очередным этапом будет построение 100-кубитного квантового компьютера.

Квантовые исследования активно ведутся на многих научно-практических площадках. Так, на базе МГТУ имени Н. Э. Баумана построен комплекс по производству сверхпроводниковых квантовых процессоров для российских интегральных схем. На площадках МИСИС и РКЦ разработаны цифровые модели управления квантовыми вы-

числениями через обычный компьютер, которые позволяют адаптировать переход от кремниего к квантовому компьютеру.

Ресурсы кремниевых компьютеров на сегодня почти исчерпаны, поэтому квантовые технологии активно внедряются в информационную инфраструктуру. В первую очередь внимание уделяется проблемам устойчивости и безопасности данных, которые служат новым активом хакеров в интернет-пространстве.

Глобальный ландшафт киберугроз постоянно меняется и требует постоянного совершенствования инструментов защиты информационной инфраструктуры. Квантовые вычисления не всегда могут надежно защитить данные, т. к. кибермошенники также работают в квантовом поиске и ищут способы взлома квантовых систем. Идет технологическая квантовая война, в которой определится лидер данного пространства.

Сегодня хакеры уже тестируют некоторые технологии активного несанкционированного вторжения. Приведем примеры:

– квантовый взлом – технология, основанная на шумочувствительности квантовых компьютеров, что дает возможности мошенникам применять квантовый шум и проникать с его помощью за периметр, чтобы саботировать итерации, дезорганизовывать работу компании или сервиса;

– квантовый вредоносный ПО, основанный на кубитах и запрограммированный для работы с квантовыми схемами, что ведет к искажениям в вычислениях, ошибкам, сбоям работы системы;

– кибератаки на цепочку поставок у самих разработчиков, то есть, хищение разработок по квантовой тематике, извлечение конфиденциальных материалов из облачных квантовых вычислительных платформ.

Так действуют кибермошенники в квантовой сфере. Поэтому необходимо уже сегодня искать возможности усиления защиты квантовыми алгоритмами. Есть примеры применения на практике некоторых алгоритмов постквантовой криптографии, обладающих высокой устойчивостью. Алгоритмы приведены в таблице 1.

Представленные в таблице 1 алгоритмы сегодня успешно адаптированы и внедрены в работу систем безопасности, эксплуатируемых различными компаниями. Но это не дает возможности решить все проблемы, так как из-за постоянного развития и появления новых технологических решений, вредоносных программ и способов проникновения за периметр требуется комплексный подход к решению вопросов цифровой безопасности. Анализ устойчивости представленных алгоритмов показывает, что они не абсолютно устойчивы к квантовому воздействию, поэтому нужен принципиально другой подход к построению цифровой защиты периметра.

Одним из вариантов является построение квантово-безопасной сети, в которой устанавливаются долгосрочная защита данных и конфиденциальное взаимодействие между контрагентами. При этом рекомендуется применять гибридные криптографические системы, основанные на традиционной шифрографии и дополненные постквантовой криптографией.

Другой способ обеспечения безопасной коммуникации – использование архитектурной схемы с нулевым доверием, в рамках которой ни один из пользователей не имеет возможности автоматического доступа в среду без непрерывной аутентификации с квантовыми генераторами случайных чисел с непредсказуемыми ключами. В такой ситуации получаем объединение постквантовой биометрической безопасности и усиление доступа посредством квантовых вычислений. Безопасные квантовые сети могут быть внутри периметра дополнительно сегментированы с распределением полномочий

между пользователями для доступа в различные секторы. Такой подход исключит горизонтальное перемещение любого пользователя внутри цифровой среды.

Таблица 1. Алгоритмы постквантового шифрования в практике компаний

Криптографический метод	**Основа безопасности**	**Квантовое сопротивление**	**Сильные стороны**	**Проблемы**	**Приложения в реальном мире**
Решетчатая криптография	Сложность задач на решётках SVP, CVP	Высокая устойчивость	Эффективный для шифрования и подписи, масштабируемый	Ключи большего размера, требуют тщательной реализации	Используется в квантово-безопасном TLS от Google, финалисте NIST (KYBER, DILITHIUM)
Многомерная криптография	Решение многомерных полиномиальных уравнений	Устойчивый (с оптимизацией)	Высокоскоростное шифрование, небольшие подписи	Больший размер ключа, сложная расшифровка	Безопасность интернета вещей, облегченное шифрование
Криптография на основе хэша	Безопасность криптографических хэш-функций	Сильное сопротивление	Проверенная безопасность, простота реализации	Ограниченное повторное использование ключа, только для подписей	Постквантовые цифровые подписи (XMSS, SPHINCS+)
Криптография на основе кода	Сложность декодирования случайных линейных кодов	Высокая устойчивость	Очень надежная система безопасности, хорошо изученная	Большие открытые ключи, медленное шифрование	Защищенная электронная почта, квантово-безопасный обмен ключами
Криптография на основе изогении	Изогении эллиптической кривой	Умеренное сопротивление	Небольшие размеры ключей, эффективные для обмена ключами	Относительно новые потенциальные уязвимости	Протоколы обмена ключами (SIDH, SIKE)
Квантовое сопротивление симметричного ключа	Ключи большего размера для AES, SHA	Требуется 2-кратный размер ключа	Эффективный для шифрования, уже используемый	Требуется удвоить длину ключа для обеспечения безопасности	AES-256, SHA-3 для квантовобезопасного шифрования

Источник: [25].

Итак, современные технологии, опирающиеся на законы квантовой физики, будут определять суперпозиции и устойчивость критической информационной инфраструктуры среди основных конкурентов и привлекать в свои сервисы максимальное количество пользователей. Дополнительное усиление инфраструктуры постквантовыми алгоритмами шифрования и безопасными квантовыми сетями коммуникаций и передачи конфиденциальных данных позволят гарантировать сохранение коммерческой тайны и работоспособность сервисов, максимально защитить их пользователей.

Проблемы кибербезопасности информационной инфраструктуры становятся вопросами государственного значения и требуют подключения уполномоченных специализированных структур для защиты национальных сервисов и систем в информационном пространстве. В результате появляется возможность дополнительного усиления и максимального охвата защитой всего информационного национального пространства.

Таким образом, кибербезопасность нового времени – это симбиоз передовых инновационных технологий и стратегий перехода к новой квантовой эпохе, которая в прогнозируемом будущем десятилетии кардинально изменит современный информационный ландшафт. Квантовое превосходство, к которому сегодня стремятся как государства, так и отдельные крупные корпорации, будет моделировать позицию своего разработчика в мировом интернет-пространстве и определять его влияние на происходящие процессы.

Цифровая среда будущего должна быть не только защищенной, но и абсолютно устойчивой к внешним вторжениям и безотказно работать. В этой связи переход к квантово-устойчивым коммуникациям, постквантовой криптографии и алгоритмам шифрования позволит гарантировать сохранность данных, работоспособность цифровых сервисов и платформ.

Заключение

Квантовые вычисления и квантовые сети сегодня уже не гипотетические перспективы, а реальная действительность. Достижение исследовательскими группами квантового превосходства произойдет примерно через 5–7 лет. Превентивные меры, которые применяют разработчики при проектировании систем информационной защиты, уже включают в себя некоторые инструменты и подходы квантовой физики.

Кибермошенники также ведут работы по тестированию квантовых сетей и вычислений на предмет устойчивости, организуя массовые утечки даже зашифрованных данных из сервисов компаний.

Российская критическая информационная инфраструктура последние 3 года испытывает колоссальное давление со стороны кибермошенников, поэтому ей требуется помощь для поддержания ее работоспособности на уровне специализированных государственных структур (ГосСОПКА). Помимо включения в национальную систему защиты на уровне предприятий и организаций должны быть внедрены постквантовые инструменты защиты данных и введена ответственность сотрудников за утечки конфиденциальной информации.

Литература

1. Кибератаки на российские компании в 2024 году. Аналитический отчет компании SOLAR. – URL: https://rt-solar.ru/analytics/reports/5320/ (дата обращения: 22.02.2025).

2. Штеренберг, С. И. Обеспечение безопасности на высокоуровневой среде Windows / С. И. Штеренберг, Г. С. Бударный, Р. Р. Ахметов // Региональная информатика

(РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. – Санкт-Петербург, 2022. – С. 585–586.

3. Большие данные на ВЭФ-2024. – URL: https://technosuveren.ru/bolshie-dannye-na-vjef-2024/ (дата обращения: 23.02.2025).

4. Штеренберг, С. И. Методика обеспечения безопасности доменных систем доверенной зоны / С. И. Штеренберг, Г. С. Бударный, И. В. Чумаков // Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. – Санкт-Петербург, 2022. – С. 621–625.

5. Баландин, Ю. А. Кибербезопасность и информационная безопасность. Демаркация правовых категорий / Ю. А. Баландин // Правовая политика и правовая жизнь. 2023. № 3. – С. 260–260.

6. Горев, А. И. Кибератаки: некоторые подходы к системному анализу / А. И. Горев, Е. Г. Горева // Математические структуры и моделирование. 2023. № 1 (69). – С. 110–116.

7. Карпенко, И. Н. О связи утечки персональных данных с показателями кибербезопасности / И. Н. Карпенко // Инженерный вестник Дона. 2024. № 9. – URL: file:///C:/Users/Gilian/Downloads/o-svyazi-utechki-personalnyh-dannyh-s-pokazatelyami-kiberbezopasnosti.pdf (дата обращения: 20.02.2025).

8. Кибербезопасность 2025: тренды, риски и ключевые решения. – URL: https://arppsoft.ru/news/experts/18184/ (дата обращения: 20.02.2025).

9. Плотников, А. В. О достижении технологического суверенитета в контексте обеспечения экономической безопасности России в условиях санкций / А. В. Плотников, В. А. Плотников // Экономика и управление. 2024. Т. 30, № 8. – С. 987–998.

10. Плотников, В. А. Постсанкционный экономический рост в России: аспекты экономической безопасности / А. В. Плотников, В. А. Плотников // Экономика Северо-Запада: проблемы и перспективы развития. 2024. № 3 (78). – С. 173–179.

11. Ревенков, П. В. Атаки на цифровой профиль клиента в условиях функционирования экосистем / Ревенков П. В., Францев В. В., Бердюгин А. А., Чебарь А. Г. // The 2023 Symposium on Cybersecurity of the Digital Economy – CDE'23. Сборник трудов VII Международной научно-технической конференции. – Иннополис, 2024. – С. 98–101.

12. Ревенков, П. В. Экосистемы: преимущества платформенных моделей, особенности построения и сопутствующие киберриски / П. В. Ревенков, В. В. Францев, А. А. Бердюгин, А. Г. Чебарь // Банковское дело. 2022. № 1. – С. 65–72.

13. Федотова, Г. В. Технологии защиты информационных ресурсов в сети интернет / Г. В. Федотова, Ю. А. Капустина, Е. В. Анянова // Национальные интересы: приоритеты и безопасность. 2024. Т. 20, № 10 (439). – С. 1858–1873.

14. Гельфанд, А. М. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры / А. М. Гельфанд, В. В. Сигачева, А. В. Архипов, Л. К. Сиротина // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. – С. 21–27.

15. Беликова, К. М. Место криптографии в обеспечении компьютерной (кибер-) безопасности и охране информации о технологиях стратегического и опережающего развития в контексте защиты научно-технических достижений в странах БРИКС / К. М. Беликова // Юридические исследования. 2021. № 9. – С. 22–62.

16. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ. Available from:

https://www.consultant.ru/ document/cons_doc_LAW_220885/ (дата обращения: 20.02.2025).

17. Федотова, Г. В. Вопросы кибеобезопасности цифровых финансовых сервисов / Г. В. Федотова, Е. Р. Орлова, И. Е. Бочарова // Информационные технологии и вычислительные системы. 2022. № 2. – С. 37–45.

18. Artur, K. Ekert. Quantum Cryptography Based on Bell's Theorem // Phys. Rev. Lett. 1991. Vol. 67, no. 6. – Pp. 661–663.

19. An integrated space-to-ground quantum communication network over 4,600 kilometres / Y. A. Chen, Q. Zhang, T. Y. Chen [et al.] // Nature. 2021. № 589. – Pp. 214–219.

20. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. 2018. Vol. 16, № 5. – Pp. 38–41.

21. Strong Quantum Computational Advantage Using a Superconducting Quantum Processor / Yulin Wu [et al.] // Physical Review Letters / American Physical Society. 2021. № 127. – URL: https://physics.aps.org/featured-article-pdf/10.1103/physrevlett.127.180501 (дата обращения: 04.03.2025).

22. Quantum supremacy using a programmable superconducting processor. F. Arute, K. Arya, R. Babbush [et al.] // Nature. 2019. № 574. – Pp. 505–510. – URL: https://doi.org/10.1038/s41586-019-1666-5 (дата обращения: 04.03.2025).

23. Антипенко, А. Л. Проблема реализма в современной квантовой механике / А. Л. Антипенко // Философия науки и техники. 2016. Т. 21, № 2. – С. 34–64.

24. Баргатин, И. В. Запутанные квантовые состояния атомных систем / И. В. Баргатин, Б. А. Гришанин, В. Н. Задков // Успехи физических наук. 2001. Т. 171, № 6. – С. 625–647.

25. Quantum Computing Cybersecurity 2025 (Complete Guide). – URL: https://www.geeksforgeeks.org/quantum-computing-cybersecurity/ (дата обращения: 05.03.2025).

Поступила в редакцию 21 марта 2025 г.
Принята 8 апреля 2025 г.

UDC 004.65

DOI: 10.21779/2500-1930-2025-40-3-7–19

Information Infrastructure Cybersecurity under Quantum Superiority

Yu. A. Kapustina[1], G. V. Fedotova[2]

[1] Ural State Forestry University; Russia, 620100, Yekaterinburg, Siberian tract, 37; kapustina_bu@mail.ru;

[2] Federal Research Center "Informatics and Management" RAS; Russia, 119333, Moscow, Vavilov st., 44, bldg. 2; g_evgeeva@mail.ru

Abstract. The global development of geopolitical confrontations and the growing technological superiority of some countries threaten the Russian information infrastructure, which is constantly subjected to attacks by cyber fraudsters from the territories of unfriendly countries. The growth and expansion of the variety of cyber attacks constantly tests the stability of the information security sys-

tem operated in the current period. The high import dependence of the Russian digital space on foreign software has proven the vulnerability of the Russian digital infrastructure after the departure of foreign suppliers of software and technologies in 2022. Obviously, the activity of fraudsters and the emergence of new types of malware require intensified search and funding for fundamentally different technological solutions to counter external unauthorized access to the information space.

Quantum research, which is being carried out today by advanced technology corporations and national jurisdictions, is a new stage in the development of public digitalization. The opportunities that the second quantum revolution opens up for the world simultaneously discredit cryptographic approaches to encryption and infrastructure protection, providing new tools to promote and improve the information infrastructure.

The authors draw conclusions, emphasizing the demand for prompt integration of quantum achievements into existing systems to maintain stability and security of the digital environment.

Keywords: information infrastructure, digital environment, security, fraudsters, hackers, cybersecurity, resilience, digital perimeter protection, malware, data.

Received 21 March, 2025
Accepted 8 April, 2025