Научный журнал КубГАУ, №205(01), 2025

УДК 004.056.55:351
5.2.2. Математические, статистические и инструментальные методы в экономике

СОВРЕМЕННЫЕ СПОСОБЫ ОПТИМИЗАЦИИ ДАННЫХ НА ГОСУДАРСТВЕННОЙ СЛУЖБЕ (ВНЕДРЕНИЕ ИНСТРУМЕНТОВ ХЭШИРОВАНИЯ)

Барановская Татьяна Петровна, доктор экон. наук, профессор, Заведующая кафедрой системного анализа и обработки информации
e-mail: bartp_2@mail.ru
ФГБОУ ВО «Кубанский государственный аграрный университет», Краснодар, Российская Федерация, ул. Калинина, 13

Тахумова Оксана Викторовна, к.э.н., доцент кафедры системного анализа и обработки информации
e-mail: takhumova@yandex.ru
ФГБОУ ВО «Кубанский государственный аграрный университет», Краснодар, Российская Федерация, ул. Калинина, 13

Агаларова Ангелина Аркадьевна, обучающаяся факультета управления
ФГБОУ ВО «Кубанский государственный аграрный университет», Краснодар, Российская Федерация, ул. Калинина, 13

Маркушина Ангелина Васильевна, обучающаяся факультета управления
ФГБОУ ВО «Кубанский государственный аграрный университет», Краснодар, Российская Федерация, ул. Калинина, 13

Рассматривается вопрос о необходимости расширения исследований и методов внедрения систем хеширования на государственной службе. Авторами поднимается вопрос о необходимости правого, теоретического и практического развития данного инструмента в системах управления государственной информацией. Представлена оценка эффективности применения технологии хеширования в российской государственной службе, приведена практика интегрирования в таких странах, как США, Япония, Китай, Норвегия. Обосновано, что проактивный подход к внедрению и адаптации технологий хеширования имеет стратегическое значение для обеспечения национальной безопасности и повышения доверия граждан к органам власти в цифровой век.

Ключевые слова: ХЕШИРОВАНИЕ, ГОСУДАРСТВЕННАЯ СЛУЖБА, РЕГИОНАЛЬНОЕ УПРАВЛЕНИЕ, IT ТЕХНОЛОГИИ, АНТИКОРРУПЦИОННАЯ

UDC 004.056.55:351
5.2.2. Mathematical, statistical and instrumental methods in economics

MODERN WAYS TO OPTIMIZE DATA IN THE PUBLIC SERVICE (IMPLEMENTATION OF HASHING TOOLS)

Tatiana Petrovna Baranovskaya, Doctor of Economics, Professor, Head of the Department of System Analysis and Information Processing
e-mail: bartp_2@mail.ru
Kuban State Agrarian University, Krasnodar, Russian Federation, Kalinina str., 13

Takhumova Oksana Viktorovna, PhD in Economics, Associate Professor of the Department of System Analysis and Information Processing
e-mail: takhumova@yandex.ru
Kuban State Agrarian University, Krasnodar, Russian Federation, Kalinina str., 13

Agalarova Angelina Arkadyevna, a student at the Faculty of Management
Kuban State Agrarian University, Krasnodar, Russian Federation, Kalinina str., 13

Angelina Vasilyevna Markushina, a student at the Faculty of Management
Kuban State Agrarian University, Krasnodar, Russian Federation, Kalinina str., 13

The issue of the need to expand research and methods of implementing hashing systems in the public service is being considered. The authors raise the issue of the need for the legal, theoretical and practical development of this tool in government information management systems. An assessment of the effectiveness of the use of hashing technology in the Russian civil service is presented, and the practice of integration in countries such as the USA, Japan, China, and Norway is presented. It is proved that a proactive approach to the introduction and adaptation of hashing technologies is of strategic importance for ensuring national security and increasing citizens' trust in government in the digital age.

Keywords: HASHING, PUBLIC SERVICE, REGIONAL MANAGEMENT, IT TECHNOLOGIES, ANTI-CORRUPTION POLICY, BIG DATA.

Введение. Все больше и больше современных технологий приводит государственную службу к необходимости формирования цифровой среды. Хеширование — это метод преобразования данных любого размера, например, текста, чисел, файлов, в строку фиксированной длины. Этот процесс позволяет значительно упростить и ускорить обработку информации, делая ее более доступной и удобной для использования. Использование такого инструмента стало новым началом не только в передачи информации, но и в целях сохранения ее целостности и защищенности. Хеширование обеспечивает высокий уровень безопасности данных, защищая их от несанкционированного доступа и изменений, что особенно важно в условиях современного цифрового мира.

Этот процесс становится все более актуальным и неизбежным в условиях стремительного развития информационных технологий. Цифровые платформы, которые давно приобрели повсеместный характер, заменили большие архивы и бюрократические требования к информации. В поисках оптимизации процессов получения и передачи информации общество пришло к новым инструментам – таким как хеширование. На данный момент тема хеширования данных на государственной службе малоизучена и не освещена в должной мере, что вынуждает обсуждать ее и стараться внедрять эти инструменты в работу органов.

Изучение таких инструментов обработки данных крайне важный объект исследований, поскольку управление данными на государственной службе затруднено рядом проблем:

– большие массивы данных, растущие с ежедневной интенсивностью не успевают обработать сотрудники;

– обучение автоматических систем затрудняется вопросами квалификации кадров и безопасностью данных;

– необходимость оптимизации данных в сжатых кодированных видах: строки, блоки данных, шифрованные ключи и т.п..

Методы исследования. Используются разнообразные оценочные инструменты, как теоретический анализ разных взглядов на процесс «хеширование» и инструменты анализа статистических показателей. В работе анализируется данные СМИ, исследования маркетинговых агентств, данные некоторых ведомств и данные опроса сотрудников ведомств региональных органов Краснодарского края.

Для проведения массовой политики хеширования данных на государственной службе необходимо чётко понимать ее основные этапы и элементы (рис. 1).

Рисунок 1 – Основные этапы хеширования данных

Когда необходимо получение данных, пересчёт хеша и сопоставление его с сохранённым хешем подтверждает отсутствие взлома. Именно такой вид контроля позволяет уменьшить коррупционные риски в работе государственных служащих и сформировать прозрачную систему подачи данных. Стратегия хеширования данных в России включает

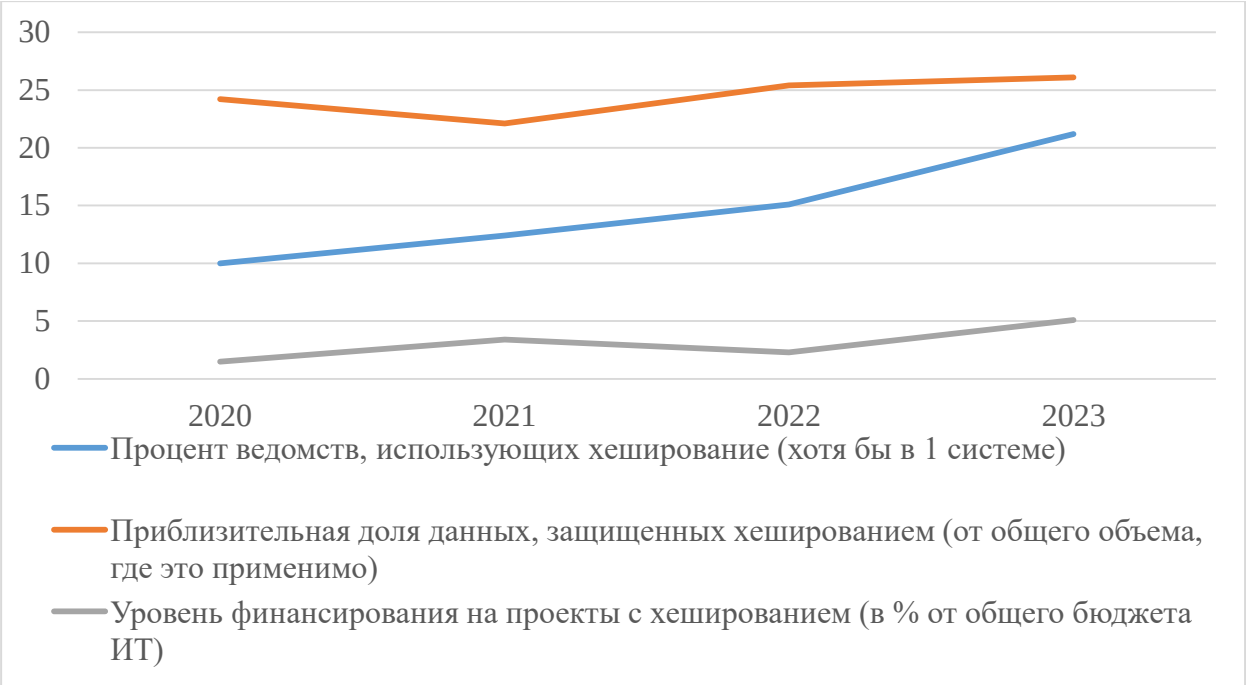
использование наших собственных криптографических стандартов. Одним из таких стандартов является ГОСТ Р 34.11-2012, также известный как функция «Стрибог». Этот стандарт представляет собой хэш-функцию, которая может работать с любым набором двоичных символов и широко применяется в компьютерных методах криптографии.

Кроме того, для хеширования данных в России используется и более новый стандарт — ГОСТ 34.11-2018. Этот стандарт описывает алгоритм вычисления хеш-функции «Стрибог». Процесс работает следующим образом: сначала сообщение произвольной длины разбивается на блоки размером 512 бит. Если необходимо, блоки дополняются до нужного размера. Затем эти входные данные преобразуются в хеш-код фиксированной длины — либо 256, либо 512 бит. Таким образом, независимо от исходного размера данных, на выходе мы получаем хеш-код определенной длины, что обеспечивает надежную защиту информации.

Помимо используемых в России стандартов хеширования, на международном уровне используются также другие методы кодирования, обладающие рядом преимуществ перед своими аналогами (SHA256, MD5). Преимущества таких методов в основном открывается в объёме информации и в скорости данного процесса.

Результаты исследования. Процесс хеширования в российском сегменте начался ещё в 2010 годах, когда внедрение цифровых инструментов стало частью тяжелой работы IT специалистов по обработке массивов данных, которые «движутся» в процессе государственного управления.

Применение данного процесса на государственной службе пока не нашло своего колоссального места, однако уже стало внедрятся в их деятельность. На рисунке 2 представлены данные статистического анализа применения хеширования работе государственных органов власти РФ,



*составлено авторами на основе источников 1,2,3

Рисунок 2 – Статистика применения технологии хеширования в российской государственной службе

Мы можем наблюдать важную динамическую линию которой отмечается нестабильное финансирование данного процесса и малый рост внедрения данной технологии в работу ведомств. Технология хеширования информации столкнулась с проблемами как обеспечения кадрами специалистами ИТ, так и проблемы в обучении персонала возможностям работы с такими шифрованными данными.

Однако, опыт других стран показывает большую интенсивность внедрения систем хеширования в работу органов государственной власти, мы рассмотрим опыт таких IT гигантов как Япония, Китай, США и Норвегия. Именно эти страны сильнее всего вносили изменения в свои государственные органы власти в процессе их информатизации и цифровизации. На рисунке 3 представлены данные сравнения представленных ранее показателей в других странах в сравнении с Российскими данными.

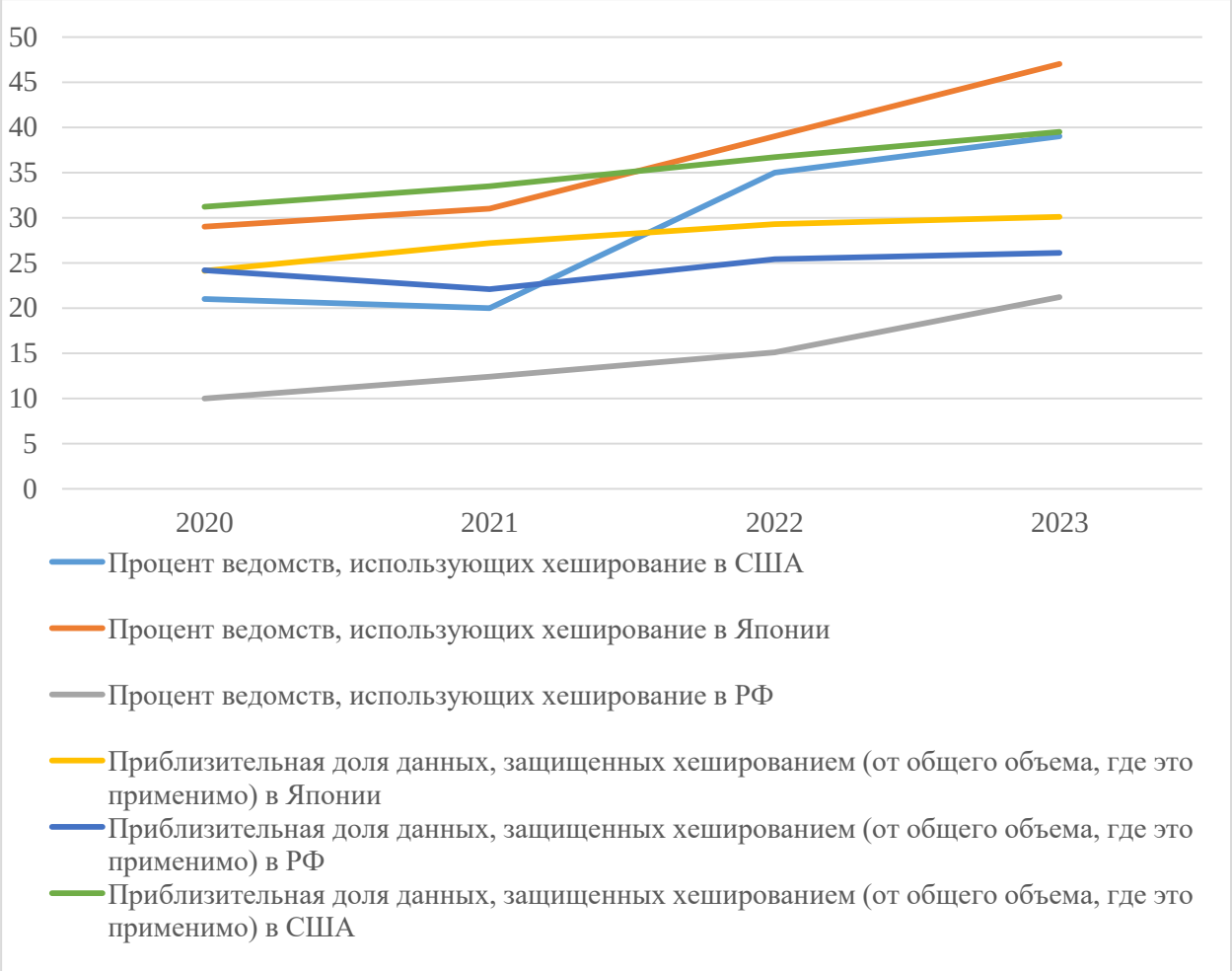


Рисунок 2 – Показатели опыта внедрения хеширования в органах государственной власти других стран

Динамически, отмечается, что наиболее интенсивный рост показателей внедрения хеширования в работу ведомств был в Японии – страна стала быстрее внедрять эти инструменты. Это подчеркивает стремительность, с которой японские государственные структуры взялись за освоение хеширования, что свидетельствует о высоком приоритете, придаваемом цифровой безопасности и эффективности. Однако, важно отметить, что этот быстрый темп внедрения сопровождался использованием уже устаревших на международном рынке протоколов шифрования. Это может говорить о том, что, несмотря на амбициозные цели, Япония, возможно, временно прибегла к более доступным, хотя и

менее современным технологиям, что в перспективе может потребовать модернизации используемой инфраструктуры.

Схожую интенсивность имеет опыт РФ, Российские власти стали внедрять эти решения в работу органов статистики и экономики регионов после 2020 года активнее (период цифровизации в пандемию). Россия, столкнувшись с необходимостью, ускоренной цифровизации, особенно в период пандемии, также продемонстрировала активное внедрение хеширования. Этот процесс коснулся, прежде всего, органов, занимающихся статистикой и экономикой регионов, что свидетельствует о стратегическом подходе к защите и управлению данными, критически важными для принятия экономических и управленческих решений.

Несмотря на то, что Япония показывает наибольшие показатели использования хеширования в своих ведомствах, объем хешированной информации в США оказывается значительно выше. Это указывает на то, что, хотя Япония и активно внедряет хеширование, США, благодаря более раннему старту и более развитой инфраструктуре, обрабатывают и защищают гораздо большие объемы данных, используя эту технологию. Технология хеширования пришла в США еще в 1995 году, когда появился первый протокол SHA-1, ставший прародителем для множества современных ключей шифрования хеша. Раннее внедрение и разработка собственных стандартов позволили США накопить значительный опыт и базу данных, что объясняет их лидерство в объеме обрабатываемой информации. Современные технологии стали важной частью управления в США, заменив обычные технологии хранения информации. Это подчеркивает, что в США хеширование не просто внедряется, а является частью фундаментальной перестройки системы управления и хранения данных на цифровой основе, что делает ее более эффективной и безопасной.. Опыт США сильно изменился за 20 лет и сейчас хеширование

нашло свое отражение в разных сферах государственного управления (рис. 3).

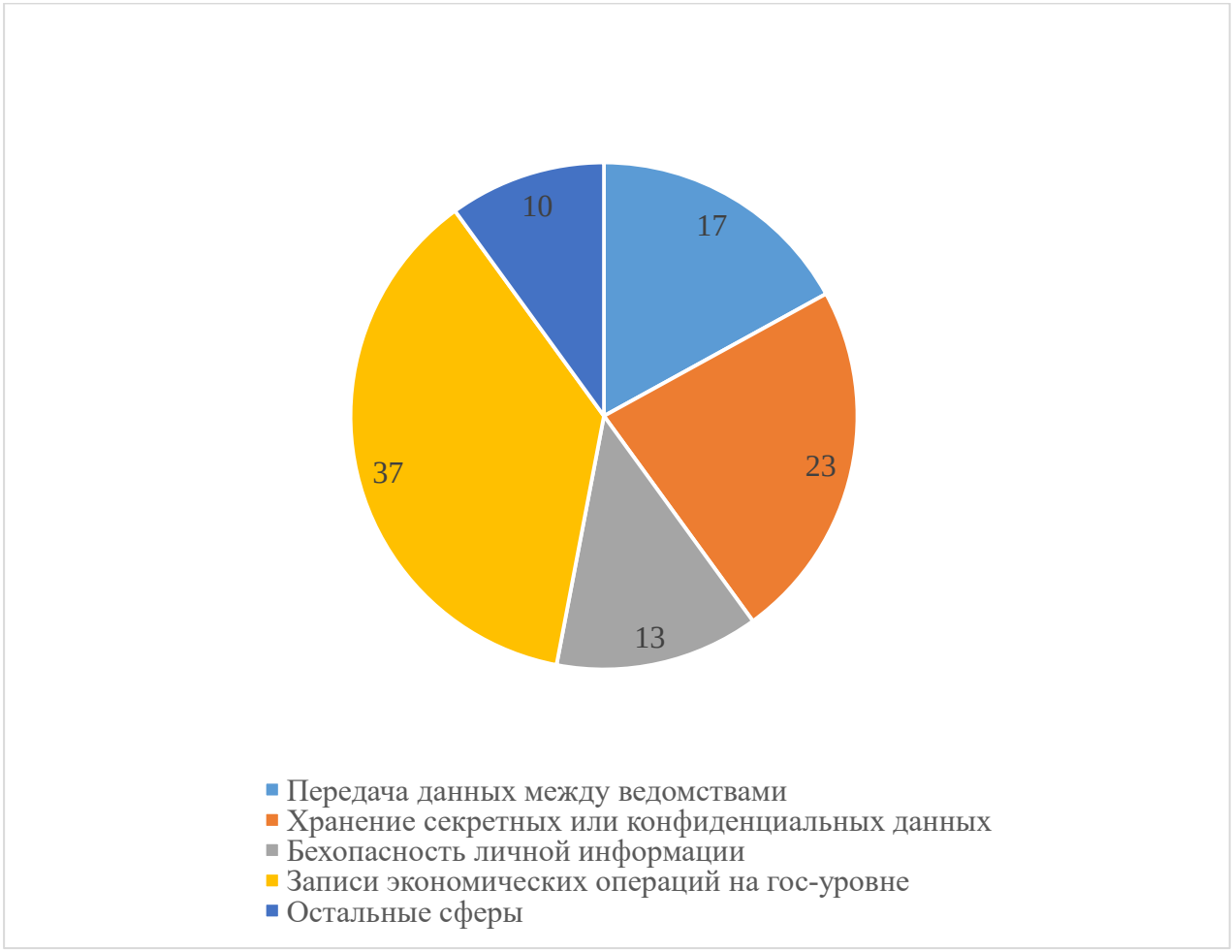


Рисунок 3 – Основные направления использования технологии хеширования в органах государственной власти США

Органы власти США сталкиваются с множеством проблем, которые вынуждают постоянно совершенствовать такую систему как хеширование, сейчас наиболее острыми проблемами стали:

– недостаток объема данных кодирования, для переноса специфической информации;

– устаревшие протоколы безопасности на государственном уровне;

– наличие бюрократических барьеров переноса данных.

Несмотря на эти проблемы, в области хеширования США является одной из «эталонных» стран в данном направлении, в отличии от Японии. Известно, что в Японии стандартом для хэш-функций является JIS X 5057-2, который является переводом ISO 10118-2. При этом использование SHA-1 описано как стандартная хэш-функция JIS с 2018 года. Интересным является, что начало своей системы хеширования Япония брала от опыта США, однако смогла создать свои уникальные кодификаторы. Уникальность системы хеширования в Японской модели заключается в ее особенной архитектуре.

В отличии от классической ISO системы, хеширование в Японии происходит не по циклическому типу, а по блочному формату – данные передаются в несколько блоков и каждый из блоков хеширует свою часть информации (схоже с технологией блокчейн). Такая многоуровневая защита данных при хешировании позволяет создавать более прозрачную и контролируемую систему передачи данных на государственной службе.

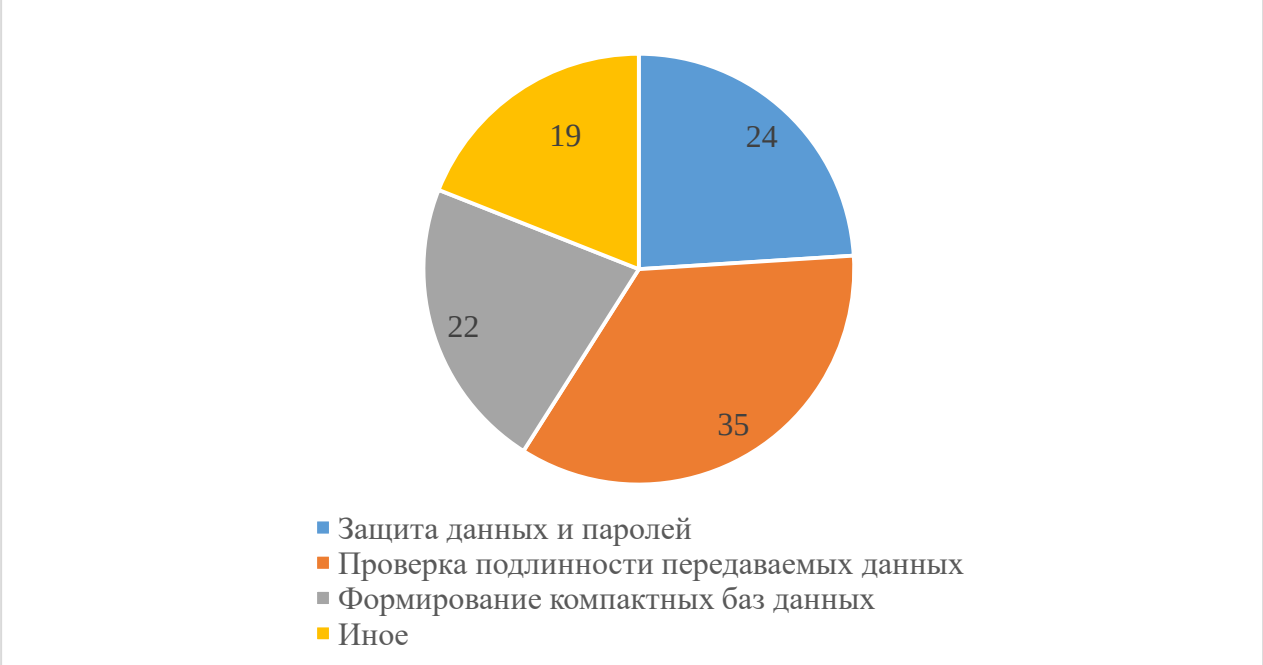


Рисунок 4 – Направления использования хеширования в государственных органах власти Японии

В Японии использование технологии хеширования нашло свое место сильнее всего в защите целостности данных, передаваемых медду ведомствами и в системах управления быстрой передачей информации. Сильная экономическая и технологическая политика государства потребовала роста эффективности подлинности данных при их хешировании. Сейчас, важной проблемой в Японской модели хешировани является устаревшие инструменты ISO которые тяжело синергируют с новыми автоматизированными системами. Руководство Японии ставит приоритетной задачу увеличения объема сжатой информации и усиления технологий блок-чейн не только в экономической среде.

Обратившись к анализу данных ведомств и учреждений в РФ, а также используя данные маркетинговых агентств и СМИ, а также опросив IT специалистов государственных органов Краснодарского края, мы можем отметить, что наиболее яркими и сложными проблемами (барьерами) в применении систем хеширования являются следующими:

1 Серверное старение: в ряде ведомств и учреждений серверная база построена на старой архитектуре и не способна выдерживать новые ключи шифрования или новые процессы сжатия информации. Такие проблемы приводят к изменению конечного результата: недостаточная качественность дешифрации полученных данных. Это означает, что даже при успешном хешировании данных, их последующая обработка и интерпретация могут быть затруднены из-за устаревшего оборудования;

2 Недостаток специалистов обслуживания инструментов хеширования: множественные массивы данных, приходящие в органы, требуют частой и многоуровневой оценки: оценка качества и количества информации, анализ направлений и скорости распространения данных, а также иных ее показателей. Недостаток специалистов не позволяет расширить или увеличить объем обработки данных и хешировать большую

часть из них. Это приводит к тому, что значительная часть информации остается незащищенной и уязвимой для внешних угроз;

3 Не до конца нормированная система контроля за хешированной информацией: система хеширования не однообразна, и модели шифрования используются в рамках удобства каждого ведомства – такие различия создают проблему в едином контроле за ее потоками. Необходимо создание единых стандартов хеширования информации на государственной службе и формирование потоковых информационных центров (в которых бы проводился анализ проходящих массивов данных). Это позволит обеспечить более высокий уровень безопасности и контроля за информацией, а также упростит процесс обмена данными между различными ведомствами.

Это лишь наиболее острые проблемы, которые отмечаются специалистами ведомств, но их список неисчерпаем, поскольку цифровое пространство развивается крайне быстро. В условиях стремительного роста объема данных и увеличения числа киберугроз, необходимость внедрения современных технологий хеширования становится все более острой. Государственные органы должны активно работать над преодолением вышеуказанных барьеров, чтобы обеспечить надежную защиту информации и эффективное функционирование цифровой среды.

Выводы и предложения. В рамках исследования нам удалось сделать соответственные вывод о том, что несмотря на довольно обширный опыт стран гигантов IT и опыт РФ система хеширования государственной информации по-прежнему требует доработок.

Нельзя однозначно сказать о необходимости использования опыта конкретной страны или использовании их протоколов, однако можно констатировать факт опыта успешного внедрения технологии в США и в Японии. Для РФ такой опыт стал пока предметом противоречий и новых требований в развитии как образовательный среды, так и кадровой

политики. Сейчас острым остается вопрос не только старения серверов и объемности информации, но и низкой доли специалистов, обладающих навыками работы с данной системой.

По мнению авторов, российской системе хеширования данных в государственном управлении не хватает самобытности и использования собственных моделей протоколирования цифровых данных. Необходимо использовать современные стандарты для преодоления барьеров и формирования стабильной системы хеширования данных. Внедрение хеширования должно быть частью комплексной стратегии цифровизации государственного управления, учитывающей не только технические аспекты, но и организационные, а также образовательные.

Для этого необходимо сформировать программы обучения специалистов, разработать единые стандарты и протоколы, а также обеспечить соответствующее финансирование и технологическое оснащение. Это позволит не только повысить безопасность данных, но и оптимизировать рабочие процессы, повысив эффективность государственного управления в целом. Проактивный подход к внедрению и адаптации технологий хеширования данных на государственной службе имеет стратегическое значение для обеспечения национальной безопасности и повышения доверия граждан к органам власти в цифровой век.

Список литературы :

1 Федеральная служба государственной статистики [электронный ресурс]: https://rosstat.gov.ru/

2 Тинькофф Журнал [электронный ресурс]: https://journal.tinkoff.ru/

3 Bits.media — первый русскоязычный информационный сайт и форум о криптовалютах [электронный ресурс]: https://bits.media/

4 World Statistics — International statistics [электронный ресурс]: https://world-statistics.org/

5 Stack Overflow [электронный ресурс]: https://stackoverflow.co/

References:

1 Federal State Statistics Service [electronic resource]: https://rosstat.gov.ru /

2 Tinkoff Magazine [electronic resource]: https://journal.tinkoff.ru /

3 Bits.media — the first Russian-language information website and forum about cryptocurrencies [electronic resource]: https://bits.media/

4 World Statistics — International statistics [electronic resource]: https://world-statistics.org /

5 Stack Overflow [electronic resource]: https://stackoverflow.co/