ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME - 2

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME - 2

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

ФОРМАЛЬНАЯ ВЕРИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ

Хамроева Азиза Хошимовна
магистр СОП БГТУ

Аннотация. Формальная верификация криптографических протоколов является одним из ключевых направлений современной информационной безопасности. Данный подход основан на строгом математическом анализе корректности протоколов и проверке таких свойств, как конфиденциальность, аутентификация и целостность данных. Методы формальной верификации включают моделирование состояний системы, проверку моделей (model checking) и доказательство теорем (theorem proving), что позволяет выявлять потенциальные уязвимости и атаки на ранних этапах разработки. Одной из наиболее распространённых моделей является модель Долева–Яо, которая описывает возможности злоумышленника в сетевой среде. В современных исследованиях активно применяются автоматизированные инструменты, такие как ProVerif, AVISPA и Tamarin, обеспечивающие анализ сложных криптографических протоколов. Особое внимание уделяется масштабируемости методов и их применению в новых областях, включая блокчейн и постквантовую криптографию. Несмотря на значительные достижения, остаются проблемы, связанные с вычислительной сложностью и ограничениями формальных моделей. Тем не менее, формальная верификация остаётся надёжным инструментом повышения безопасности цифровых систем.

Ключевые слова: формальная верификация, криптографические протоколы, проверка моделей, доказательство теорем, модель Долева–Яо, безопасность, ProVerif, AVISPA, Tamarin

Annotatsiya. Kriptografik protokollarni formal verifikatsiya qilish zamonaviy axborot xavfsizligining muhim yo‘nalishlaridan biri hisoblanadi. Ushbu jarayon protokollarning mantiqiy to‘g‘riligini, maxfiylik, autentifikatsiya va yaxlitlik kabi xavfsizlik xususiyatlarini qat’iy matematik modellar asosida tekshirishni nazarda tutadi. Formal verifikatsiya usullari, jumladan model tekshirish (model checking), teoremalarni isbotlash (theorem proving) va avtomatlashtirilgan analiz vositalari orqali amalga oshiriladi. Bu yondashuvlar kriptografik protokollarda yuzaga kelishi mumkin bo‘lgan zaifliklar va hujum ssenariylarini oldindan aniqlash imkonini beradi. Ayniqsa, Dolev–Yao modeli asosida ishlab chiqilgan abstrakt tizimlar keng qo‘llanilib, ular orqali dushman modeli va aloqa kanallari nazorat qilinadi. Zamonaviy tadqiqotlarda ProVerif, AVISPA va Tamarin kabi vositalar yordamida murakkab protokollarni avtomatik tahlil qilish keng rivojlanmoqda. Shuningdek, formal metodlarning rivojlanishi kvantga chidamli kriptografiya va

ISSN 3030-3907

blokcheyn texnologiyalarida qo‘llanilish istiqbollarini kengaytirmoqda. Shu bilan birga, formal verifikatsiya hisoblash murakkabligi va modellashtirishning to‘liqligi bilan bog‘liq muammolarni ham o‘z ichiga oladi. Ushbu yo‘nalishdagi ilmiy izlanishlar protokollarni yanada ishonchli va xavfsiz qilishga xizmat qiladi.

Kalit so‘zlar: formal verifikatsiya, kriptografik protokollar, model checking, theorem proving, Dolev–Yao modeli, xavfsizlik, ProVerif, AVISPA, Tamarin

Annotation. Formal verification of cryptographic protocols represents a critical domain in modern information security, focusing on the rigorous validation of protocol correctness through mathematical and logical methods. This approach ensures essential security properties such as confidentiality, authentication, and integrity. Formal verification techniques include model checking, theorem proving, and automated reasoning tools, which enable the systematic detection of vulnerabilities and potential attack vectors. The Dolev–Yao model is widely adopted as an abstraction for adversarial capabilities in communication networks. Advanced tools such as ProVerif, AVISPA, and Tamarin have significantly improved the automation and scalability of protocol analysis. Recent developments highlight the application of formal methods in emerging areas like blockchain systems and post-quantum cryptography. However, challenges remain in terms of computational complexity and the expressiveness of formal models. Despite these limitations, formal verification continues to play a vital role in enhancing the reliability and security of cryptographic systems.

Keywords: formal verification, cryptographic protocols, model checking, theorem proving, Dolev–Yao model, security, ProVerif, AVISPA, Tamarin

ВВЕДЕНИЕ.

В условиях стремительного развития цифровых технологий и глобальной цифровизации общества вопросы обеспечения информационной безопасности приобретают критическое значение. Криптографические протоколы лежат в основе защищённого обмена данными в распределённых системах, включая электронную коммерцию, облачные вычисления, системы электронного правительства и коммуникационные сети. Они обеспечивают такие фундаментальные свойства, как конфиденциальность, целостность, аутентификация и неотказуемость.Несмотря на использование криптографически стойких алгоритмов, уязвимости часто возникают не на уровне примитивов (например, шифров или хэш-функций), а на уровне логики самих протоколов. Исторически известно множество атак, таких как атаки повторного воспроизведения (replay attacks), атаки посредника (man-in-the-middle) и нарушения аутентификации, которые стали возможны из-за ошибок проектирования протоколов. Это подчеркивает необходимость

ISSN 3030-3907

строгого анализа корректности их работы.Формальная верификация представляет собой математически обоснованный подход к проверке корректности систем, позволяющий доказать выполнение заданных свойств безопасности во всех возможных сценариях. В отличие от эмпирического тестирования, формальные методы обеспечивают полноту анализа, исключая влияние человеческого фактора и ограниченности тестовых наборов.Целью данного исследования является анализ методов формальной верификации криптографических протоколов, выявление их преимуществ и ограничений, а также оценка их роли в обеспечении современной кибербезопасности. Для достижения поставленной цели решаются следующие задачи: рассмотрение основных подходов к формальной верификации, анализ инструментальных средств, выявление типичных уязвимостей и сравнительная оценка методов.Формальная верификация криптографических протоколов основывается на различных методологических подходах, каждый из которых обладает своими особенностями и областью применения.Одним из первых направлений являются логические методы, среди которых особое место занимает BAN-логика (Burrows–Abadi–Needham). Этот подход основывается на формализации убеждений участников протокола и анализе того, какие знания они получают в процессе обмена сообщениями. BAN-логика позволяет выявлять логические ошибки в аутентификации, однако её ограниченность заключается в абстрактности и невозможности учета всех аспектов поведения злоумышленника.Другим важным методом является моделирование состояний (model checking). В рамках этого подхода протокол представляется в виде конечной системы переходов состояний, а затем автоматически проверяется выполнение заданных свойств безопасности. Model checking позволяет систематически исследовать все возможные сценарии выполнения протокола, включая действия потенциального нарушителя. Однако основной проблемой является «взрыв состояний», который ограничивает масштабируемость метода.Теоремное доказательство (theorem proving) представляет собой наиболее строгий подход, основанный на использовании математических доказательств корректности протоколов. В этом случае свойства безопасности формулируются в виде теорем, которые затем доказываются с использованием логических систем. Данный метод обеспечивает высокую точность, но требует значительных усилий и высокой квалификации исследователя.Символьный анализ, также известный как модель Долева–Яо, рассматривает криптографические операции как идеальные «черные ящики» и анализирует протокол на уровне символических представлений.

ISSN 3030-3907

Этот подход широко используется благодаря своей эффективности и автоматизируемости.

Для практической реализации формальной верификации применяются специализированные инструменты. ProVerif основан на символьном анализе и использует процессные исчисления для проверки свойств безопасности. AVISPA предоставляет платформу для автоматического анализа протоколов с использованием различных бэкендов. Tamarin сочетает символьный анализ и теоремное доказательство, обеспечивая гибкость и выразительность. Scyther ориентирован на быстрый поиск атак и анализ протоколов в ограниченных моделях.Каждый из этих инструментов реализует собственную модель злоумышленника, чаще всего основанную на предположении о полной контролируемости сети (модель Долева–Яо), что позволяет анализировать широкий спектр атак.Анализ методов формальной верификации показывает, что они эффективно выявляют широкий спектр уязвимостей криптографических протоколов. Среди наиболее распространённых проблем можно выделить нарушение аутентификации, утечку секретной информации, атаки повторного воспроизведения и ошибки в управлении ключами.Логические методы, такие как BAN-логика, позволяют выявлять ошибки в интерпретации сообщений участниками протокола. Однако их ограниченность проявляется в неспособности учитывать сложные сценарии атак.Методы model checking демонстрируют высокую эффективность при обнаружении логических ошибок и атак, включая man-in-the-middle. Они позволяют автоматически находить контрпримеры, иллюстрирующие нарушение свойств безопасности. Тем не менее, при увеличении сложности протокола наблюдается экспоненциальный рост числа состояний.Теоремное доказательство обеспечивает наиболее строгие гарантии безопасности. Оно позволяет формально доказать, что протокол удовлетворяет заданным свойствам при любых условиях. Однако данный подход требует значительных временных и интеллектуальных ресурсов.Символьный анализ является компромиссным решением, сочетая автоматизацию и достаточную точность. Он широко применяется в современных инструментах и позволяет эффективно анализировать реальные протоколы.В качестве примера можно рассмотреть анализ протокола обмена ключами. Формальная верификация позволяет выявить возможность атаки посредника в случае отсутствия аутентификации сторон. Добавление механизмов проверки подлинности (например, цифровых подписей) устраняет данную уязвимость, что подтверждается результатами анализа.Сравнительный анализ методов формальной верификации

ISSN 3030-3907

показывает, что ни один из них не является универсальным решением. Логические методы удобны для концептуального анализа, но ограничены в выразительности. Model checking обеспечивает автоматизацию и полноту перебора состояний, однако страдает от проблем масштабируемости. Теоремное доказательство предоставляет максимальную строгость, но требует значительных усилий. Символьный анализ представляет собой наиболее практичный подход для анализа реальных протоколов.Современные тенденции развития формальной верификации направлены на интеграцию различных методов с целью повышения эффективности и точности анализа. Например, комбинированные подходы позволяют использовать преимущества символьного анализа и теоремного доказательства.Перспективным направлением является применение формальной верификации в автоматизированных системах разработки, включая DevSecOps-практики. Это позволяет выявлять уязвимости на ранних этапах жизненного цикла программного обеспечения. Кроме того, развитие вычислительных мощностей и алгоритмов оптимизации способствует преодолению проблемы взрыва состояний.Особое значение формальная верификация приобретает в контексте новых технологий, таких как Интернет вещей, блокчейн и квантовая криптография, где ошибки в протоколах могут иметь критические последствия. Таким образом, формальная верификация криптографических протоколов является неотъемлемым инструментом обеспечения информационной безопасности. Её применение позволяет существенно повысить надежность систем и минимизировать риски, связанные с эксплуатацией уязвимостей. В условиях роста киберугроз дальнейшее развитие и внедрение формальных методов становится приоритетной задачей научного и инженерного сообщества.

Формальная верификация криптографических протоколов представляет собой одно из наиболее значимых и интенсивно развивающихся направлений современной теории информационной безопасности, основанное на применении строгих математических методов для доказательства корректности функционирования протоколов в условиях потенциально враждебной среды. В отличие от традиционных методов тестирования, которые способны выявлять лишь ограниченное множество ошибок, формальная верификация позволяет гарантировать выполнение заданных свойств безопасности при всех возможных сценариях взаимодействия, включая активные атаки злоумышленника. Научная база данного направления сформирована на пересечении таких дисциплин, как дискретная математика, логика, теория алгоритмов и криптография, а

ISSN 3030-3907

ключевые концепции опираются на строго формализованные модели вычислений и коммуникаций. Одной из фундаментальных моделей анализа является модель Долева–Яо, в рамках которой злоумышленник рассматривается как всесильный участник сети, способный перехватывать, модифицировать и подделывать сообщения, за исключением нарушения криптографических примитивов, считающихся идеальными. Такая абстракция позволяет сосредоточиться на логике протокола и выявлении концептуальных уязвимостей, не углубляясь в детали конкретных криптоалгоритмов.Среди основных методов формальной верификации выделяются проверка моделей и доказательство теорем, каждая из которых имеет свои преимущества и ограничения. Проверка моделей основана на систематическом переборе состояний системы с целью выявления нарушений заданных свойств, что делает её особенно эффективной для автоматизированного анализа конечных систем, однако она сталкивается с проблемой взрыва состояний при увеличении сложности протокола. Доказательство теорем, напротив, позволяет работать с бесконечными пространствами состояний и более абстрактными моделями, но требует значительных интеллектуальных усилий и высокой квалификации исследователя. В последние десятилетия значительное развитие получили автоматизированные инструменты, такие как ProVerif, AVISPA и Tamarin, которые позволяют существенно упростить процесс анализа и сделать его доступным для практического применения в разработке реальных протоколов. Эти системы используют различные формальные языки и логические исчисления, включая π-исчисление и его производные, для описания взаимодействий между участниками протокола и проверки свойств безопасности, таких как секретность, аутентификация и устойчивость к атакам повторного воспроизведения.Научные исследования показывают, что формальная верификация играет ключевую роль в выявлении критических уязвимостей даже в широко используемых протоколах, таких как SSL/TLS, Kerberos и протоколы электронной коммерции, что подтверждает необходимость её применения на ранних этапах проектирования систем. Особое значение приобретает интеграция формальных методов в жизненный цикл разработки программного обеспечения, что соответствует современным концепциям secure-by-design и позволяет существенно снизить риски эксплуатации уязвимостей в реальных условиях. В последние годы наблюдается расширение области применения формальной верификации, включая анализ протоколов в распределённых системах, облачных вычислениях, Интернете вещей и блокчейн-технологиях, где требования к безопасности особенно высоки.

ISSN 3030-3907

При этом возникают новые вызовы, связанные с масштабируемостью методов, необходимостью учёта вероятностных и временных аспектов, а также интеграцией формальных моделей с реальными криптографическими примитивами, обладающими неидеальными свойствами.Несмотря на достигнутый прогресс, остаются нерешённые проблемы, включая высокую вычислительную сложность анализа, ограниченную выразительность некоторых формальных языков и необходимость компромисса между точностью модели и её вычислительной реализуемостью. Тем не менее, современные научные работы подтверждают, что дальнейшее развитие формальных методов, включая использование искусственного интеллекта и автоматического синтеза доказательств, открывает перспективы создания более надёжных и безопасных криптографических протоколов. Таким образом, формальная верификация выступает не только как инструмент анализа, но и как фундаментальная методология обеспечения доверия в цифровых системах, что делает её неотъемлемой частью современной научной и инженерной практики в области кибербезопасности.

Формальная верификация криптографических протоколов в современной научной парадигме рассматривается как строго обоснованный метод анализа безопасности, базирующийся на математических моделях и логических доказательствах корректности взаимодействий в распределённых системах, и её значимость подтверждается широким спектром фундаментальных и прикладных исследований в области криптографии и теории вычислений. В научной литературе, включая работы Roger Needham и Michael Schroeder, а также более поздние исследования Gavin Lowe, продемонстрировано, что даже протоколы, считавшиеся корректными, могут содержать скрытые уязвимости, выявляемые исключительно с помощью формальных методов, что стало важным аргументом в пользу их обязательного применения. Существенный вклад в развитие теоретической базы внесла модель Dolev–Yao model, предложенная Danny Dolev и Andrew Yao, которая формализует поведение злоумышленника и задаёт основу для анализа протоколов в условиях полного контроля над коммуникационной средой, при этом предполагая идеальность криптографических примитивов, что позволяет сосредоточиться на логических аспектах протокольного взаимодействия.Научно обоснованный анализ показывает, что методы формальной верификации, такие как model checking и theorem proving, обладают различной эпистемологической природой, но в совокупности обеспечивают высокую степень достоверности результатов, поскольку первый метод ориентирован на автоматизированный перебор состояний

ISSN 3030-3907

системы и выявление контрпримеров, тогда как второй направлен на построение строгих математических доказательств корректности, что подтверждается исследованиями в области формальных методов, связанными с такими концепциями, как process calculus и π-calculus, предложенный Robin Milner, который широко используется для моделирования взаимодействующих процессов в криптографических протоколах. Практическая значимость формальной верификации подтверждается применением автоматизированных инструментов, таких как ProVerif, AVISPA и Tamarin, которые позволяют проводить анализ протоколов с учётом различных моделей атак, обеспечивая выявление нарушений свойств конфиденциальности и аутентификации, что подтверждено многочисленными публикациями в рецензируемых журналах и материалах международных конференций по информационной безопасности.Дополнительные исследования демонстрируют, что формальная верификация сыграла ключевую роль в анализе широко используемых протоколов, включая SSL/TLS и Kerberos, где были выявлены критические уязвимости, ранее не обнаруженные традиционными методами тестирования, что подтверждает необходимость интеграции формальных методов в жизненный цикл разработки программного обеспечения в соответствии с принципами secure-by-design. В научных работах также подчёркивается, что развитие вычислительных мощностей и алгоритмов автоматизации способствует расширению применимости формальной верификации к более сложным системам, включая распределённые вычисления, облачные инфраструктуры и технологии блокчейн, однако остаются нерешённые проблемы, связанные с экспоненциальным ростом пространства состояний и ограниченной выразительностью формальных моделей при описании реальных криптографических примитивов, обладающих вероятностными характеристиками. Современные направления исследований, отражённые в трудах ведущих учёных и организаций, указывают на перспективность интеграции методов машинного обучения и автоматического синтеза доказательств для повышения эффективности анализа, что открывает новые возможности для создания надёжных криптографических систем. Таким образом, совокупность научно обоснованных источников подтверждает, что формальная верификация является неотъемлемым инструментом обеспечения безопасности, позволяющим не только выявлять уязвимости, но и формировать теоретически гарантированные свойства защищённости протоколов, что делает её критически важной для развития современной цифровой инфраструктуры.Формальная верификация криптографических

ISSN 3030-3907

протоколов, как подтверждается анализом современной научной литературы, представляет собой фундаментально обоснованный и практически значимый подход к обеспечению информационной безопасности, основанный на строгих математических и логических методах. В отличие от эмпирических способов тестирования, формальные методы позволяют не только обнаруживать отдельные ошибки, но и доказывать корректность протоколов в рамках заданных моделей угроз, что обеспечивает более высокий уровень доверия к цифровым системам. Использование таких моделей, как Dolev–Yao model, а также формальных языков, включая π-calculus, создаёт теоретическую основу для анализа взаимодействий в распределённых системах. Практическая реализация этих подходов через инструменты, такие как ProVerif, AVISPA и Tamarin, подтверждает их эффективность в выявлении уязвимостей в реальных протоколах, включая SSL/TLS и Kerberos. Несмотря на существующие ограничения, связанные с вычислительной сложностью и необходимостью упрощения моделей, дальнейшее развитие формальных методов, включая автоматизацию доказательств и интеграцию с современными технологиями, открывает значительные перспективы для повышения надёжности и устойчивости криптографических систем. В совокупности это позволяет рассматривать формальную верификацию не только как инструмент анализа, но и как ключевой элемент методологии проектирования безопасных протоколов в условиях возрастающих киберугроз.

СПИСОК ЛИТЕРАТУРЫ:

1. Danny Dolev, Andrew Yao. On the Security of Public Key Protocols. IEEE Transactions on Information Theory, 1983.
2. Roger Needham, Michael Schroeder. Using Encryption for Authentication in Large Networks of Computers. Communications of the ACM, 1978.
3. Gavin Lowe. Breaking and Fixing the Needham–Schroeder Public-Key Protocol Using FDR. Tools and Algorithms for the Construction and Analysis of Systems, 1996.
4. Robin Milner. Communicating and Mobile Systems: The π-Calculus. Cambridge University Press, 1999.
5. Blanchet B. Automatic Verification of Cryptographic Protocols: A Tutorial. Foundations and Trends in Privacy and Security, 2016.
6. Armando A. et al. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. CAV, 2005.
7. Meier S., Schmidt B., Cremers C., Basin D. The Tamarin Prover for the Symbolic Analysis of Security Protocols. CAV, 2013.

ISSN 3030-3907

8. Rescorla E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley, 2001.
9. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. Prentice Hall, 2002.
10. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.