УДК 316.776; 004.056.5

Е.А. Гончар ассист.;
А.Н. Мущук ассист. (БГТУ, г. Минск)

БЕЗОПАСНОСТЬ *NDN*: КРИПТОГРАФИЧЕСКИЕ ПОДХОДЫ ДЛЯ ЗАЩИТЫ КОНТЕНТНО-ОРИЕНТИРОВАННЫХ СЕТЕЙ ОТ УГРОЗ

NDN (Named Data Networking) – это архитектура сети, которая ориентирована на данные, а не на их местоположение. В отличие от традиционных IP-сетей, где коммуникация основана на адресах устройств (IP-адресах), в NDN фокус смещается на сами данные и их имена. Это позволяет создавать более гибкие, безопасные и эффективные сети, особенно в условиях современного интернета, где запросы на контент играют ключевую роль.

Основные цели *NDN*:

1. Ориентация на контент: В *NDN* пользователи запрашивают данные по их именам, а не по адресам устройств. Это упрощает доступ к информации, особенно в условиях, когда данные могут быть доступны из множества источников.

2. Повышение безопасности: Данные в *NDN* подписываются на уровне архитектуры, что обеспечивает их аутентичность и целостность.

3. Эффективность: *NDN* позволяет кэшировать данные на промежуточных узлах сети, что снижает нагрузку на серверы и ускоряет доставку контента.

4. Устойчивость к изменениям топологии сети: поскольку данные идентифицируются по именам, а не по местоположению, сеть может адаптироваться к изменениям, таким как отказ узлов или изменение маршрутов.

Принципы работы *NDN*:

1. Именование данных:

– каждый фрагмент данных в *NDN* имеет уникальное имя, которое используется для его запроса и идентификации. Имена иерархичны и могут быть структурированы, например: */video/lectures/ndn/intro*;

– имена позволяют запрашивать данные независимо от их местоположения.

2. Два типа пакетов:

– *Interest* (Запрос): Пакет, который отправляется пользователем для запроса данных. В нем указывается имя данных;

– *Data* (Данные): Пакет, который содержит запрошенные данные и их имя. Данные подписываются производителем, что гарантирует их подлинность.

3. Маршрутизация на основе имен: в *NDN* маршрутизация осуществляется на основе имен данных, а не *IP*-адресов(*Internet Protocol*). Узлы сети хранят таблицы, которые связывают имена данных с возможными путями их получения.

4. Кэширование данных: каждый узел в *NDN* может кэшировать данные, которые он передает. Это позволяет повторно использовать данные для последующих запросов, что снижает нагрузку на сеть и ускоряет доставку.

5. Безопасность на уровне данных: каждый пакет данных в *NDN* подписывается производителем. Это позволяет проверять подлинность и целостность данных на любом этапе их передачи.

6. Отсутствие привязки к местоположению: поскольку данные запрашиваются по именам, а не по адресам, *NDN* не зависит от конкретного местоположения данных. Это делает сеть более устойчивой к изменениям и отказоустойчивой [1,2].

NDN бросает вызов устоявшейся "*push*" модели передачи данных, выбирая вместо этого "*pull*" дизайн, при котором данные доставляются исключительно по явным запросам потребителей. Этот фундаментальный отход от традиционных методов вещания на основе *IP* иллюстрируется акцентом *NDN* на именованных данных в отличие от обычных адресов хоста или интерфейса. Более того, *NDN* включает криптографические механизмы, обязывающие производителей данных подписывать их содержимое цифровой подписью. Этот инновационный подход отделяет доверие к данным от доверия к объектам хранения и распространения. Поскольку *NDN* стремится превзойти существующую интернет-архитектуру на основе *TCP*/*IP (Transmission Control Protocol/ Internet Protocol)*, она требует тщательной проверки по всему спектру сценариев связи, охватывающих телекоммуникации, видеоконференции, интеллектуальные системы учета и управления.

Несмотря на свой огромный потенциал, *NDN* остается уязвимым перед проблемами, присущими новаторским дизайнам Интернета, включая восприимчивость к атакам и ограничения масштабируемости. Эти проблемы подчеркивают первостепенную важность разработки стратегий противодействия таким угрозам, как распределенные атаки типа "Отказ в обслуживании" (*DDoS – denial-of-service attack*), и устранения ограничений масштабируемости. В эпоху, когда обычных мер безопасности, таких как физическая или логическая изоляция, оказыва-

ется недостаточно, криптографические подходы приобрели известность как средство укрепления цифровых коммуникаций [3].

Криптографические методы, применяемые в *NDN*:

1. Цифровые подписи используются для подтверждения подлинности и целостности данных. Они гарантируют, что данные были созданы конкретным отправителем и не были изменены [4].

Принцип работы следующий, создается пара ключей: закрытый (для подписи) и открытый (для проверки). Отправитель вычисляет хэш данных. Хэш шифруется с использованием закрытого ключа, создавая подпись. Получатель вычисляет хэш полученных данных. Расшифровывает подпись с использованием открытого ключа. Сравнивает хэши. Если они совпадают, подпись верна. Алгоритмы: *RSA,ECDSA, EdDSA*.

2. Шифрование данных используется для обеспечения конфиденциальности данных, делая их недоступными для несанкционированного доступа. При симметричном шифровании один ключ используется для шифрования и расшифрования. Алгоритмы: *AES, ChaCha20*.

При асимметричное шифровании используется пара ключей: открытый (для шифрования) и закрытый (для расшифрования). Примеры: *RSA, ECIES*.

3. Хэширование используется для создания уникальных идентификаторов данных и проверки их целостности. Данные передаются через хэш-функцию. Результат – хэш фиксированной длины, уникальный для входных данных. Алгоритмы: *SHA-256, SHA-3, BLAKE3*.

4. Управление ключами включает генерацию, распределение, хранение и обновление ключей. Генерация ключей: создается пара ключей (закрытый и открытый). Распределение ключей: использование *PKI* или децентрализованных систем. Хранение ключей: безопасное хранение закрытых ключей. Обновление ключей: регулярная смена ключей для минимизации рисков.

5. Аутентификация подтверждает личность пользователя, а авторизация определяет уровень доступа. Пользователь предоставляет учетные данные (например, сертификат). Система проверяет права доступа.

6. Защита от атак включает предотвращение *replay*-атак, кэш-отравления и других угроз. Метки времени для предотвращения повторного использования пакетов и проверки актуальности данных.

7. Конфиденциальность имен защищает информацию, содержащуюся в именах данных. Для этого происходит шифрование имен и использование псевдонимов.

8. Децентрализованные методы, такие как блокчейн, используются для управления ключами и сертификатами [5].

9. Энергоэффективные криптографические методы предназначены для устройств с ограниченными ресурсами (*IoT – internet of things*). Легковесные алгоритмы: *SPHINCS+, Lightweight Encryption Algorithm*.

Каждый из криптографических методов играет важную роль в обеспечении безопасности *NDN*. Их комбинация позволяет создавать надежные и масштабируемые системы, защищенные от современных угроз.

Криптографические подходы в *NDN* направлены на обеспечение безопасности данных в условиях децентрализованной и ориентированной на контент архитектуры. Основные задачи – это аутентификация, целостность, конфиденциальность и защита от атак. Однако внедрение криптографии в NDN требует тщательного баланса между безопасностью и производительностью, особенно в устройствах с ограниченными ресурсами.

ЛИТЕРАТУРА

1. Гончар Е.А. Угрозы и проектирование безопасности информационноориентированных сетей (ICN) / Е.А. Гончар, Ю.А. Чистякова, А.С. Пахолко // Информационные технологии: материалы 86-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января - 12 февраля 2022 г. – Минск: БГТУ, 2022.

2. Гончар Е.А. Механизмы обеспечения безопасности в NDN / Е.А. Гончар, Н.В. Пацей // Тезисы 73-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов учащихся, студентов и магистрантов, Минск, 18-23 апреля 2022 г. [Электронный ресурс] / отв. за издание И.В. Войтов; УО БГТУ. – Минск: БГТУ, 2022.

3. Mirajkar R.R. et al. NDN Security: Cryptographic Approaches for Safeguarding Content-Centric Networking against Threats //Journal of Electrical Systems. – 2024. – Т. 20. – №. 3s. – С. 1516-1541.

4. Li B., Zheng M., Ma M. A Novel Security Scheme Supported by Certificateless Digital Signature and Blockchain in Named Data Networking //IET Information Security. – 2024. – Т. 2024. – №. 1. – С. 6616095.

5. Yang H. K., Cha H. J., Song Y. J. Secure identifier management based on blockchain technology in NDN environment //Ieee Access. – 2018. – Т. 7. – С. 6262-6268.