кущую версию с предыдущей. Этот процесс называется «поиском различий» (diffing) [1-3].

Библиотека React и фреймворк Vue примерно одинаково работают, они используют Virtual DOM. Но есть несколько отличий. По сравнению с React – Vue, напротив, использует алгоритм «обновления на месте» (in-place patching), который обновляет виртуальное DOM на месте без полного сравнения со старым состоянием.

React использует систему «подъема состояния» (state lifting) и «контекст» (context) для отслеживания изменений, тогда как Vue предоставляет систему наблюдателей (observers) и реактивных свойств (reactive properties). Vue также предлагает вычисляемые свойства (computed properties) и наблюдаемые свойства (watchers) для более удобной работы с реактивностью.

Фреймворк Angular, в отличие от библиотек Vue и React, использует Incremental DOM. Incremental DOM используется компанией Google для внутренних нужд. Его основная идея такова: «Каждый компонент компилируется в набор инструкций, которые создают DOM-деревья и непосредственно обновляют их при изменении данных». Выводом из выполненной работы является анализ использования DOM, который может быть полезен для программистов, начинающих работать с библиотекой и фреймворками, упомянутыми в докладе.

УДК 004.62

Студ. И.С. Викторович
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Беспроводные сети стали неотъемлемой частью нашей повседневной жизни, однако их уязвимость к различным видам атак, таким как перехват и взлом, представляет серьезную угрозу для безопасности передаваемой информации [1].

Для защиты информации в беспроводных сетях существуют четыре типа протоколов безопасности: WEP, WPA, WPA2 и WPA3. Базовым алгоритмом WEP являлся алгоритм RC4. Протокол WPA (Wi-Fi Protected Access) был разработан в качестве замены уязвимого протокола WEP (Wired Equivalent Privacy). WPA использовал алгоритм шифрования TKIP (Temporal Key Integrity Protocol), который был добавлен к базовому алгоритму RC4. TKIP предоставлял дополнительные механизмы безопасности, такие как динамическое изменение

ключей и контроль целостности сообщений. С появлением протокола WPA2, внедренного в стандарте IEEE 802.11i, алгоритм RC4 был заменен на более безопасный и криптостойкий алгоритм шифрования AES [1, 2]. Беспроводные сети подвержены различным угрозам извне, самыми распространёнными из которых являются такие как «Человек посередине», или Man-in-the-middle, DDOS-атаки, ложные точки доступа и другие. Усилить защиту можно при помощи программных, аппаратных и аппаратно-программных средств (WIPS-системы, Fortinet, Sophos Wireless).

В области криптографической защиты беспроводных сетей проводится множество исследований, направленных на разработку новых методов и улучшение существующих технологий – квантовая криптография, методы машинного обучения для обнаружения атак, развитие протоколов аутентификации и шифрования, защита от атак со стороны искусственного интеллекта, управление уязвимостями и стандартизация [2, 3].

ЛИТЕРАТУРА

1 Урбанович, П. П. Компьютерные сети и сетевые технологии: учеб. пособие для студ. технических спец. / П.П. Урбанович, Д.М. Романенко. – Минск: БГТУ, 2022. – 608 с.

2. Анализ безопасности Wi-Fi [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/bastion/articles/777182/ – Дата доступа: 29.03.2024.

3. Ласык, Я. Использование сетевых протоколов и стеганографии для тайной передачи информации / Я. Ласык, Д.М. Романенко, П.П. Урбанович // Информационные технологии: материалы 86-й НТК профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января – 12 февраля 2022 г. – Минск: БГТУ, 2022. – С. 158–163.

УДК 003.26

Студ. А. Н. Халалеенко, Т.С. Шишова
Науч. рук. проф., д-р техн. наук П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

МЕТОДЫ ШИФРОВАНИЯ В МОБИЛЬНЫХ УСТРОЙСТВАХ

С каждым днем все больше людей используют мобильные устройства для проведения финансовых транзакций, обмена конфиденциальной информацией и доступа к личным данным. Вместе с этим увеличивается и риск кибератак, направленных на кражу чувствительных данных, в том числе банковских реквизитов, личных сообщений и фотографий. Поэтому, разработка и применение надежных