Университет ИТМО, факультет программной инженерии и компьютерной техники

Двухнедельная отчётная работа по «Информатике»: аннотация к статье

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Дата прошедшей лекции | Номер прошедшей лекции | Название статьи/главы книги/видеолекции | Дата публикации (не старше 2021 года) | Размер статьи (от 400 слов) | Дата сдачи |
| 11.09.2024 | 1 | Логические и арифметические операции в системе счисления фибоначчи и их применение в вычислительных системах | 26.11.2022 | ~2002 | 25.09.2024 |
| 25.09.2024 | 2 | Анализ корректирующей способности кодов Рида-Соломона в системах передачи данных | 12.04.2021 | ~1728 | 09.10.2024 |
| 09.10.2024 | 3 | Обработка естественного языка | 26.05.2021 | ~2010 | 23.10.2024 |
| 23.10.2024 | 4 | Протоколы защищенной передачи сообщений | 30.05.2022 | ~1651 | 06.11.2024 |
|  | 5 |  |  |  |  |
|  | 6 |  |  |  |  |
|  | 7 |  |  |  |  |

Выполнил(а) Мельник Ф.А. , № группы *P3106* , оценка

Фамилия И.О. студента не заполнять

|  |
| --- |
| **Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т.п.)**  https://www.elibrary.ru/item.asp?id=48676919 |
| **Теги, ключевые слова или словосочетания (минимум три слова)**  ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СЕТЕВАЯ БЕЗОПАСНОСТЬ, СИСТЕМЫ ОБМЕНА СООБЩЕНИЯМИ, ОБМЕН МГНОВЕННЫМИ СООБЩЕНИЯМИ, КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ, АСИММЕТРИЧНОЕ ШИФРОВАНИЕ, ОБМЕН КЛЮЧАМИ |
| **Перечень фактов, упомянутых в статье (минимум четыре пункта)**   1. Чтобы сообщения в интернете были безопасными и никто посторонний не мог их прочитать, используют специальные протоколы, которые шифруют данные. 2. Протокол **OTR** защищает сообщения с помощью особого шифрования, которое каждый раз создает новый ключ, чтобы взломщики не могли прочитать переписку. 3. Протокол **XMPP** работает по схеме «клиент-сервер», то есть сообщения проходят через сервер, который их защищает с помощью технологий TLS и SASL. 4. Протоколы защиты разрабатывают по-разному в зависимости от задачи: иногда важна большая секретность, а иногда — скорость работы. |
| **Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)**   1. Технологий защищенной передачи данных повышает безопасность, надежность и гибкость мессенджеров и других систем связи. 2. Одноранговая архитектура не зависит от центрального сервера, что повышает надежность и устойчивость к сбоям. 3. Можно выбирать протоколы с разной степенью защиты в зависимости от ситуации, что делает технологии универсальными и удобными для пользователей. |
| **Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)**   1. Шифрование каждого сообщения с новым ключом (как в OTR и Signal) требует значительных ресурсов, что может замедлить работу устройств 2. Некоторые протоколы шифрования сложно интегрировать с другими системами, что может ограничивать их использование. 3. В одноранговых системах, как Bitmessage, нет центрального сервера для резервного копирования сообщений, поэтому данные могут быть потеряны. |
| **Ваши замечания, пожелания преподавателю *или* анекдот о программистах[[1]](#footnote-1)** |

1. Наличие этой графы не влияет на оценку [↑](#footnote-ref-1)