

Поляков О.А.

*Научный руководитель: к.т.н., доцент К.В.Макаров
Муромский институт (филиал) федерального государственного образовательного
учреждения высшего образования «Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail:xtarget.plus@gmail.com*

Корпоративный мессенджер

Оптимизация работы одна из важнейших задач любого бизнеса, производства, учреждения. На это уходит много времени, денег и сил и не всегда результат удовлетворителен.

Для того, чтобы облегчить работу организациям и разрабатывается данный мессенджер.

Главный упор идет на удобство и защищенность данных, ныне самое главное в интернете. Удобства гарантируются за счет внутренней экосистемы, а защищенность за счет сложной криптографической системы шифрования данных, скриптами от SQL-инъекций в базах данных и настройкой защиты серверной части.

Допустим вам нужно создать контент-план на полгода вперед, распределить задачи на команду со сроками сдачи. Кто-то использует таблицы в Excel, сторонние программы, дополнительно используя различные методы распределения приоритетов: Матрица Эйзенхауэра, Метод Парето и другие. Вместо всех этих громоздких шагов, лишних кликов, можно воспользоваться нашим мессенджером и создать там контент план в разделе Конструкторы -> Контент план. Затем в этот план можно будет добавить сотрудников из списка контактов, распределить задачи и открыть файлоприемник. Удобно и сотрудникам, они смогут отчитываться перед вами, не выходя из мессенджера, переключившись на диалоги.

Перейдем к защите данных. На раннем этапе разработки мы выбрали асинхронный способ шифрования данных с помощью алгоритма RSA с использованием расширенного алгоритма Евклида. Асинхронный метод подразумевает создание двух ключей: открытого и секретного. Ключи будут передаваться с помощью протокола передачи Диффи-Хеллмана.

Данные будут храниться в реляционной СУБД MySQL. Плюс данной СУБД – гибкость (легко масштабируется), высокая скорость записи и считывания, не привязанная к ключу активации, удобный интерфейс для серверов. Для защиты баз данных в первую очередь будут написана защита от SQL-инъекций, PHP-инъекций.

В серверной части все намного сложнее с защитой. Будут написаны защиты от таких распространенных видов атак как – DoS и DDos, IP-спуфинг, сетевая разведка, phishing-атаки, man-in-the-middle, внедрений скрытых серверов и угроза переполнения буфера. Для еще лучшей защиты планируется размещение серверов, а не покупка удаленных.

Разработка мессенджера сейчас находится на начальном этапе, но с каждым днем мы все ближе к ее завершению. Следующим нашим этапом будет открытое бета тестирование.

Литература

1. Э.Таненбаум, Д.Уэзеролл Компьютерные сети пятое издание 2010 год. Дата обращения 10.04.2022.