

### **Литература**

1 Муравьев, Г. Л. О прототипировании приложений с использованием диаграмм UML / Г. Л. Муравьев, В. И. Хвещук, С. В. Мухов // Инновационные технологии обучения физико-математическим и профессионально-техническим дисциплинам: материалы 14-й междунар. научно-практ. конф., Мозырь, 29 марта 2022. – С. 266–268.

**К. С. Караханова, Е. Ю. Кузьменкова**  
(ГГУ имени Ф. Скорины, Гомель)

### **РАЗРАБОТКА ДИЗАЙНА МОБИЛЬНОГО ПРИЛОЖЕНИЯ „MARIMO“ С ИСПОЛЬЗОВАНИЕМ KOTLIN, ANDROID STUDIO**

Современные мобильные приложения становятся неотъемлемой частью жизни пользователей, помогая решать повседневные задачи и поддерживать психологическое благополучие. Однако в мире, полном тревог и стресса, даже простые действия – выпить воды, размяться, позвонить другу – могут даваться с трудом. Как мотивировать человека заботиться о себе? Можно ли превратить заботу о себе в увлекательный процесс? „Marimo“ – это мобильное приложение, в котором уход за виртуальным питомцем становится метафорой самоподдержки и осознанного ухода за собой.

Приложение разработано на Kotlin с использованием среды Android Studio. Для создания пользовательского интерфейса применялся XML, а механизм SharedPreferences обеспечил сохранение данных пользователя. Обработка анимаций и изображений осуществлялась с помощью библиотеки Glide, а обновление интерфейса и механики работы с игровыми событиями реализовано через Handler и Runnable.

Приложение выполнено в жанре «тамагочи», где пользователь ухаживает за своим виртуальным другом, выполняя базовые действия: кормление, купание и игры. От регулярности этих действий зависит «уровень счастья» питомца, представленный в виде очков: чем лучше пользователь заботится о нём, тем счастливее он становится. Если игрок забывает выполнять базовые действия, питомец начинает грустить, а его показатели снижаются.

Интерфейс „Marimo“ включает три основных экрана: стартовый, игровой и экран заданий. Дополнительной возможностью приложения является система случайных заданий, направленная на развитие полезных привычек. Пользователь получает небольшие задания – выпить стакан воды, сделать разминку, прогуляться – и, выполняя их, восстанавливает ресурсы, которые позволяют заботиться о питомце. „Marimo“ – это не просто мобильная игра, а диалог с самим собой, помогающий пользователю осознать, что забота о себе – это не сложная задача, а естественный процесс, наполненный маленькими, но важными шагами к внутренней гармонии.

**А. А. Карлюк**

*(ГрГУ имени Янки Купалы, Гродно)*

## **СРЕДСТВА И МЕТОДЫ АНАЛИЗА АЛГОРИТМОВ ШИФРОВАНИЯ**

Шифрование является ключевым процессом для обеспечения конфиденциальности и целостности данных в современном мире, где информация становится одним из самых ценных активов. Учитывая рост объемов передаваемой информации и увеличение числа киберугроз, корректное использование методов шифрования стало первоначально важным для защиты личных и корпоративных данных.

Цель работы заключается в анализе теоретических уязвимостей классических алгоритмов шифрования, таких как RSA и AES, а также в исследовании атак на эти алгоритмы, основанных на возможности доступа к устройствам шифрования.

В ходе работы основное внимание уделялось атакам, основанным на теоретических слабостях алгоритма RSA. Таким как: факторизация модуля ( $n = p * q$ ) – если злоумышленник сможет разложить модуль на множители, можно вычислить приватный ключ; атака с использованием малых показателей (Low Exponent Attack) – использование маленького публичного показателя (например,  $e = 3$ ) может упростить дешифровку при определённых условиях; атака по малому модулю (Small Modulus Attack) – если размер модуля недостаточно велик, это может позволить взлом. В отношении возможности эксплуатации уязвимостей алгоритма AES, внимание акцентировалось таких криптоаналитических атаках как: дифференциальный крипто-