Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК

Новик
Анна Михайловна

Обеспечение безопасности данных пользователей мобильных устройств

АВТОРЕФЕРАТ
диссертации на соискание степени магистра техники и технологии
по специальности 1-39 80 03 Электронные системы и технологии

_____
(подпись магистранта)

Научный руководитель
Пискун Геннадий Адамович
(фамилия, имя, отчество)
Канд. техн. наук, доцент
(ученая степень, ученое звание)

_____
(подпись научного руководителя)

Минск 2021

Работа выполнена на кафедре электронной техники и технологии учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **ПИСКУН Геннадий Адамович,**
кандидат технических наук, доцент, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ПРУДНИК Александр Михайлович,**
кандидат технических наук, доцент, доцент кафедры инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «27» апреля 2021 г. года в 9^{00} часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П. Бровки, 6, корп. 1, ауд. 135, тел. 293-88-35, e-mail: kafett@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

КРАТКОЕ ВВЕДЕНИЕ

Современные технологии и мобильные устройства позволяют сделать жизнь пользователей более гибкой и доступной к информации и различным возможностям. В частности, за последние несколько лет технологии позволяют с помощью мобильного приложения оплатить коммунальные услуги, оформить кредит или открыть депозит, посмотреть курсы валют, выбрать, заказать и оплатить доставку еды, купить понравившийся товар из-за границы через интернет-магазин всего в пару кликов, заказать такси, отследить свою поездку, посмотреть расписание общественного транспорта, решить рабочие вопросы с помощью мессенджеров и электронной почты из любой страны, оплатить покупки в магазине с помощью смартфона или планшета и многое другое.

Из-за цифровизации повседневной жизни люди вынуждены задуматься о безопасности своих персональных данных. Практически каждое приложение, установленное у нас на телефоне, хранит наши персональные данные. Это могут быть номера банковских карт, информация о различных финансовых транзакциях, различные документы, доступ к которым нежелателен для посторонних, номера телефонов, адреса, фотографии. Многие приложения требуют привязки банковских карт, а соответственно такие приложения более уязвимы для злоумышленников, так как предоставляют доступ к нашим финансам.

Существует несколько способов защиты персональных данных пользователей в мобильном приложении. Это могут быть стандартные методы («Логин/Пароль», *PIN*-код, графический ключ, одноразовый *SMS*-код), биометрические методы (сканирование отпечатка пальца, распознавание по лицу, по голосу, по подписи) или комбинированные (как правило, это пара из стандартного и биометрического способов). Каждый из них имеет достоинства и недостатки. Абсолютно уникального, надёжного и простого способа на сегодняшний день нет, однако можно добиться приближённого эффекта, используя тот или иной метод в определённых условиях.

Для создания наиболее эффективного способа защиты персональных данных необходимо провести анализ имеющихся способов, сравнить их по различным критериям, выделить преимущества и недостатки, разработать новый алгоритм, основанный на результатах исследования, добавив дополнительные функции при необходимости.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время мобильные технологии значительно расширили возможности человека. Существует множество различных приложений для смартфонов и планшетов, которые привносят в нашу жизнь удобства и экономят время. Принцип работы большей части таких приложений базируется на персональных данных пользователя. Соответственно вопрос как защитить

персональные данные от злоумышленников, какой метод защиты наиболее эффективный и безопасный остаётся открытым.

Степень разработанности проблемы

Исследованиями в области обеспечения безопасности персональных данных занимаются Кухарев Г.А., Митин В., Клейнберг Дж., Тардос Э., Бхаргава А., Кормен Т., Еременко А.В., Flajolet PH., Sedgewick R, Парамонов И.В. и др.

Предложенное исследование и разработанный алгоритм направлены на повышение безопасности персональных данных и эффективности использования при разработке новых и доработке существующих методов защиты персональных данных пользователей мобильных приложений.

Цель и задачи исследования

Целью работы является разработка алгоритма защиты персональных данных пользователей мобильных приложений с дальнейшим внедрением в программный модуль, тестированием технической части и полным анализом готового алгоритма.

Поставленная цель работы определяет следующие основные задачи:

– анализ в области обеспечения безопасности данных пользователей мобильных приложений: обзор существующих способов защиты персональных данных, сравнение их по различным критериям;

– разработка алгоритма защиты персональных данных пользователей мобильных приложений, позволяющего повысить уровень сохранности персональных данных без потери в удобстве его использования;

– оценка эффективности разработанного алгоритма;

– интеграция алгоритма в программный модуль и последующим тестированием технической части;

– анализ разработанного алгоритма по различным критериям.

Теоретическая и методологическая основа исследования

В основу работы легли исследования в таких областях, как программирование мобильных приложений, безопасность персональных данных, биометрические технологии, научное программирование, алгоритмизация, математическая статистика и теория вероятности.

Информационная база исследования сформирована из научных изданий, научно-исследовательских работ, ресурсов Интернет, специализированной литературы, материалов научных изданий и статей.

Научная новизна

Научная новизна результатов работы заключается в следующем:

– разработан алгоритм защиты персональных данных пользователей мобильных приложений, который состоит из комбинированного способа защиты

и имеет функцию автоматической отправки сообщения пользователю на электронную почту в случае неверной попытки идентификации;

– предложена возможная реализация разработанного алгоритма в программном продукте для операционной системы *Android* на языке программирования *Java*.

Основные положения, выносимые на защиту

1. Анализ методов защиты персональных данных пользователя и современных мобильных приложений (использующих эти данные), позволивший установить уязвимые места во время идентификации пользователя в мобильном приложении, изучить особенности каждого метода, а так же оценить их достоинства и недостатки.

2. Алгоритм защиты персональных данных пользователей мобильных приложений, основанный на комплексном исследовании мер по защите персональных данных, позволяет повысить уровень безопасности мобильных приложений, хранящих конфиденциальную информацию, и своевременно уведомить пользователя о попытке несанкционированного доступа.

3. Оценка эффективности разработанного алгоритма в программном продукте, позволившая обозначить преимущества используемого комбинированного метода и дополнительной функции защиты в алгоритме относительно других по различным критериям.

Личный вклад

В диссертационной работе представлены материалы исследований, которые являются результатом самостоятельной работы автора. Выполнены исследования существующих методов защиты персональных данных пользователей мобильных приложений, разработан алгоритм защиты персональных данных, дана оценка эффективности нового алгоритма и проведён анализ полученных результатов.

Планирование работ, определение структуры, целей и задач исследования, обсуждение и обобщение основных научных результатов исследования проводились совместно с научным руководителем, кандидатом технических наук, доцентом Г.А. Пискуном.

Диссертационная работа выполнена самостоятельно, проверена в системе «Атиплагиат». Процент оригинальности составляет 85,21. Заимствования обозначены ссылками на публикации, указанные в «Список используемых источников»

Апробация диссертации и информация об использовании её результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на следующих конференциях: 56 и 57-я научные конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Беларусь, 2020 –

2021 г.), VII Международной научно-практической конференции (школы-семинара) молодых ученых «Прикладная математика и информатика: современные исследования в области естественных и технических наук» (г. Тольятти, Россия, 2021 г.), X Республиканской научной конференции аспирантов, магистрантов и студентов «Актуальные вопросы физики и техники» (г. Гомель, Беларусь, 2021 г.).

Опубликование результатов диссертации

Основные положения диссертации и результаты исследования изложены в 5 опубликованных работах, состоящих из 5 докладов на научных конференциях.

Структура и объём диссертации

Диссертация состоит из введения, трёх глав с краткими выводами по каждой главе, заключения и списка использованных источников.

Во **введении** обоснована актуальность выбранной темы исследования, сформулированы цели и задачи работы, показана её научная и практическая значимость. В **первой главе** проведено исследование способов хранения информации на мобильном устройстве; исследованы различные типы мобильных приложений, требующих персональных данных пользователя, а также систематизированы методы обеспечения безопасности персональных данных пользователей мобильных приложений. Во **второй главе** проведён анализ стандартных и биометрических способов защиты, разработан алгоритма защиты персональных данных, дана оценка эффективности разработанного алгоритма. В **третье главе** представлен анализ альтернативного алгоритма защиты персональных данных, разработан программный модуль на основе предложенного алгоритма, осуществлено тестирование технической часть программного модуля и проведён анализ и сравнение разработанного алгоритма в программном продукте по различным критериям.

Общий объём диссертационной работы составляет 68 страниц. Из них X страниц основного текста, 37 иллюстраций на 19 страницах, 7 таблиц на 5 страницах, список собственных публикаций из 5 наименований на 9 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное отношение к безопасности персональных данных пользователей мобильных приложений, определены основные направления исследования, даётся обоснование актуальности темы диссертационной работы, описываются цель и задачи исследования.

В **первой главе** представлена структура хранения данных в мобильных устройствах и обзор каждого из способов.

Структура хранения данных:

1. Внутренняя память: ОЗУ; ПЗУ; КЭШ-память.

2. Внешняя память: внешние носители: *Flash*-карта (*SD, microSD*), *USB* флеш-накопители, *HDD*-накопитель, *SSD*-накопитель; облачные хранилища; локальное хранение данных приложения; базы данных.

Исследован рынок мобильных приложений, использующих персональные данные. На рисунке 1 представлен график наиболее популярных категорий мобильных приложений у пользователей.

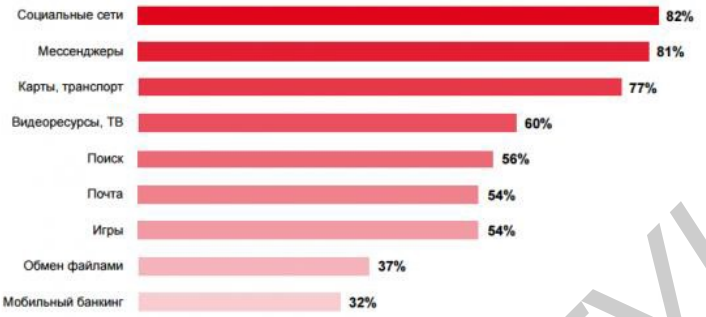

Рисунок 1 – График наиболее популярных категорий мобильных приложений у пользователей

Согласно графику, видно, что у пользователей достаточно большой спрос на приложения, требующие использования персональных данных. К ним относятся социальные сети, мессенджеры, транспорт, почта, обмен файлами, мобильный банкинг. Основные данные, которые надо защищать, это номера банковских карт, счетов, финансовые транзакции, личные переписки, адреса, номера телефонов, файловые документы, изображения.

Систематизированы основные методы защиты персональных данных на входе в приложение и на каждый из них предоставлен обзор.

Основные методы: по отпечатку пальца, по распознаванию лица, по распознаванию голоса, по подписи, по «Логин/Пароль», по графическому рисунку, по *PIN*-коду, по одноразовому *SMS*-паролю.

Согласно приведённым данным наиболее распространёнными способами защиты персональных данных в приложении являются отпечаток пальца, распознавание по лицу, пара «Логин/Пароль» и *PIN*-код.

Вторая глава посвящена разработке алгоритма, построенного на анализе стандартных и биометрических методов защиты персональных данных в мобильном приложении. Дана оценка эффективности разработанного алгоритма на основе исследования времени идентификации, вероятности успешной идентификации пользователя и применимости разработанного алгоритма на различных устройствах.

Из стандартных способов защиты можно выделить «Логин/Пароль», так как он является наиболее надёжным и позволяет «привязать» пользователя к номеру телефона или электронной почте.

Согласно анализу наиболее распространённая, простая и надёжная является биометрическая технология: идентификация по отпечатку пальца. Это связано с простотой использования и уникальностью.

На основе полученных результатов разработан алгоритм из комбинированных методов защиты: идентификация по отпечатку пальца или с помощью пары «Логин/Пароль». Помимо идентификации пользователя алгоритм выполняет обработку действий в случае неудачных попыток ввода идентификационных данных: временно блокирует возможность идентификации пользователя и отправляет на электронную почту пользователя уведомление о неудачной попытке входа и координатами мобильного устройства и временем события.

На рисунке 2 представлена блох-схема разработанного алгоритма защиты персональных данных пользователей мобильных приложений.

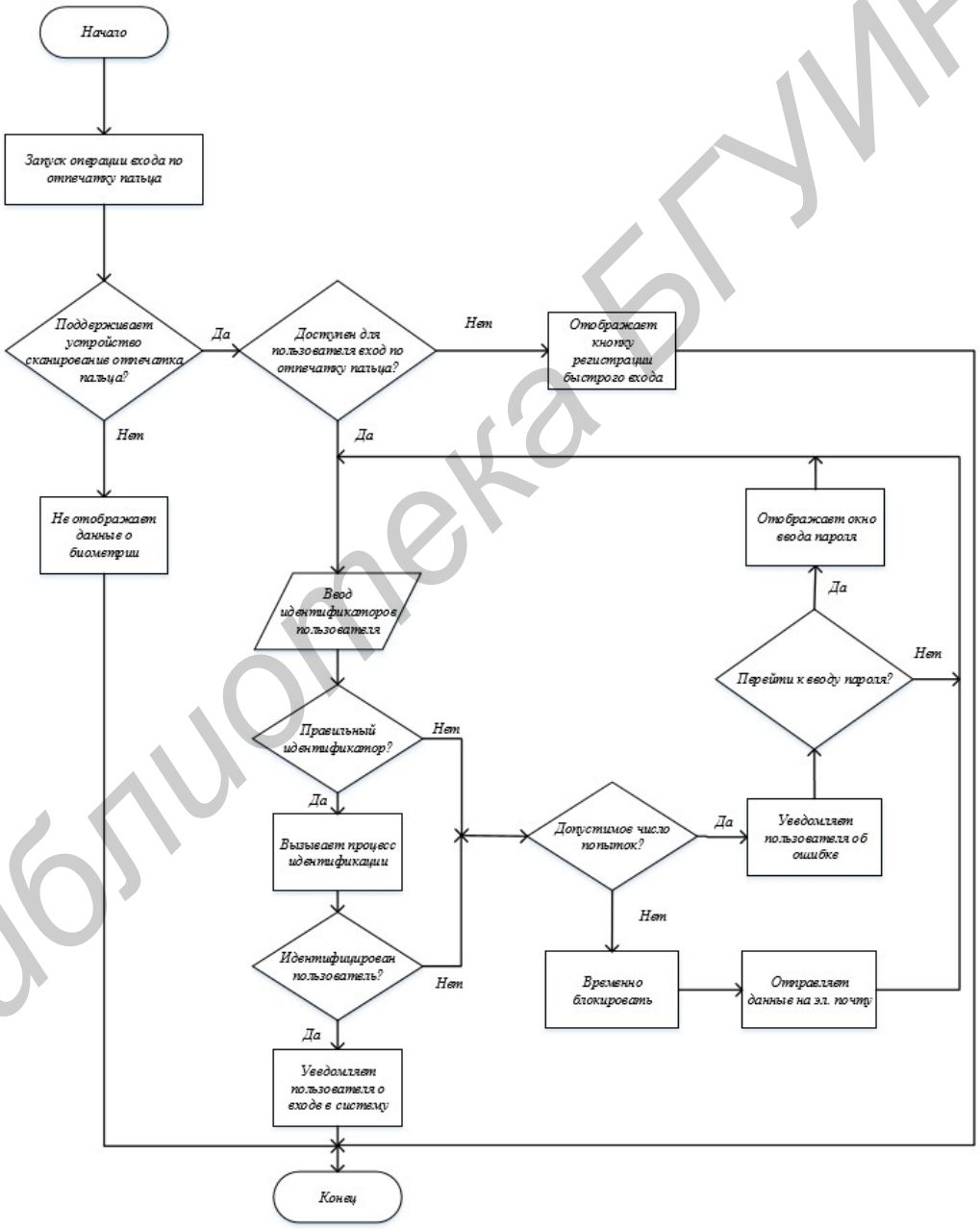

Рисунок 2 – Блок-схема алгоритма защиты персональных данных пользователя

Разработанный алгоритм включает два способа защиты: биометрический (сканирование отпечатка пальца) как основной и «Логин/Пароль» как

альтернативный. Алгоритм имеет функцию отправки информации о неудачных попытках идентификации на электронную почту пользователя, что позволяет вовремя среагировать на попытки несанкционированного доступа и предотвратить потерю персональных данных.

Третья глава посвящена оценке эффективности и безопасности идентификации альтернативного сценария защиты с разработанным. Рассмотрена возможность оптимизации программного модуля посредством использования разработанного алгоритма. Проведено тестирование технической составляющей программы по различным сценариям. Проведён анализ разработанного алгоритма в программном продукте.

Критерии анализа: скорость идентификации пользователя, безопасность идентификации, энергозатраты, техническое решение, наличие уникальности, сравнение разработанного программного продукта с альтернативным.

Объектами анализа являются:

1. Комбинированные методы защиты: отпечаток пальца и «Логин/Пароль», «Логин/Пароль» и *PIN*-код, распознавание по лицу и «Логин/Пароль», распознавание по голосу и «Логин/Пароль».

2. Отдельные (стандартные и биометрические) методы защиты: «Логин/пароль», *PIN*-код, одноразовый *SMS*-код, отпечаток пальца, распознавание по лицу, распознавание по голосу.

В таблице 1 представлены данные о среднем количестве входных данных для успешной идентификации посредством отдельных (стандартных и биометрических) методов.

Таблица 1 – Среднестатистическое количество символов для успешной идентификации пользователя

Название метода	Среднее количество входных данных, шт
Логин и пароль	9
PIN-код	4
Одноразовый *SMS*-код	4
Отпечаток пальца	1
Распознавание по лицу	1
Распознавание по голосу	1

Согласно данным из таблицы 1 наименьшее количество входных данных для успешной идентификации требуется для биометрических методов защиты персональных данных.

На рисунке 3 представлены *значения скорости идентификации* с помощью отдельных методов. Данные из графика на рисунке 3 получены в ходе испытаний и измерений средней длительности идентификации пользователя для каждого способа. Скорость в данном случае понимается как время, затраченное на ввод полных идентификаторов, необходимых для успешной идентификации.

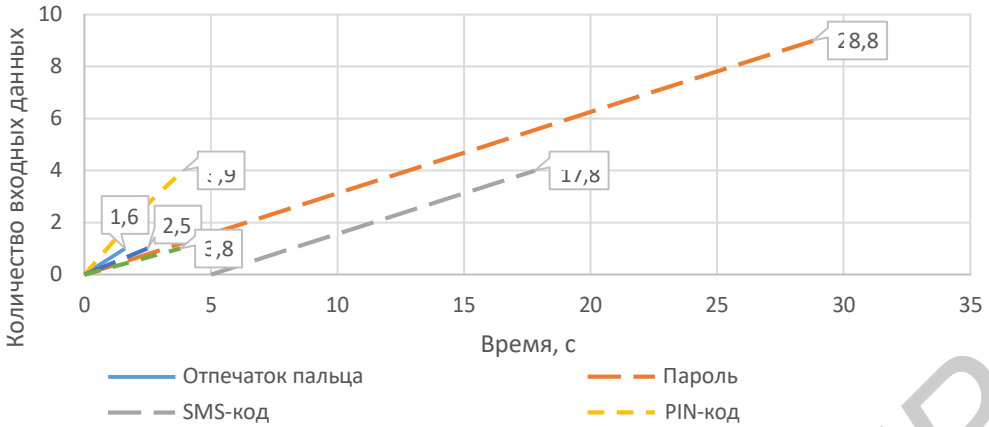

Рисунок 3 – Диаграмма времени ввода входных данных пользователем

В таблице 2 представлено общее время идентификации пользователя для рассматриваемых методов защиты.

Таблица 2 – Общее время идентификации пользователя

Методы защиты	Общее время, с
«Логин/пароль» + распознавание по голосу	32,6
«Логин/пароль» + распознавание по лицу	31,3
«Логин/пароль» + *PIN*-код	32,7
«Логин/пароль» + отпечаток пальца	30,4

Общее время – это время, которое надо потратить на идентификацию с помощью одного метода (неуспешный результат идентификации), переключение на альтернативный и идентификацию с помощью него. Наименьшее время понадобится для метода «Логин/пароль» + отпечаток пальца. Для остальных методов время увеличится на 7,2% («Логин/пароль» + распознавание по голосу), на 3% («Логин/пароль» + распознавание по лицу) и на 7,2% («Логин/пароль» + *PIN*-код). В качестве одного из способа идентификации для комбинированного метода целесообразно рассматривать «Логин/Пароль». Такое решение принято в результате исследования различных факторов, одно из его преимуществ – возможность привязать пользователя к номеру телефона или электронной почте.

Согласно полученным данным наименьшее время понадобится для ввода отпечатка пальца, а наибольшее – для ввода значений логина и пароля. При использовании пары «Логин/Пароль» в комбинированном методе время идентификации займёт от 29 секунд (в зависимости от количества и типа вводимых символов), при использовании отпечатка пальца – около 1,6 секунды. При последовательном использовании отпечатка пальца и пары «Логин/Пароль» минимальное затраченное время займёт 30,4 секунд.

Преимущество разработанного программного продукта – это наличие и комбинированной защиты, и быстрое время идентификации пользователя.

Согласно анализу *уровень безопасности идентификации* достигает до 96,7-98%. В ходе анализа безопасности идентификации пользователя были

рассмотрены различные параметры: уникальность, возможность подделать, доступность для посторонних, идентификация личности, вероятность забыть/потерять, влияние внешних факторов на процесс идентификации.

Исследование *энергозатрат* до внедрения и после внедрения разработанного программного модуля показали несущественное отличие (результат представлен на рисунке 4), что значит: использование разработанного алгоритма в программном модуле не требует дополнительной энергии.

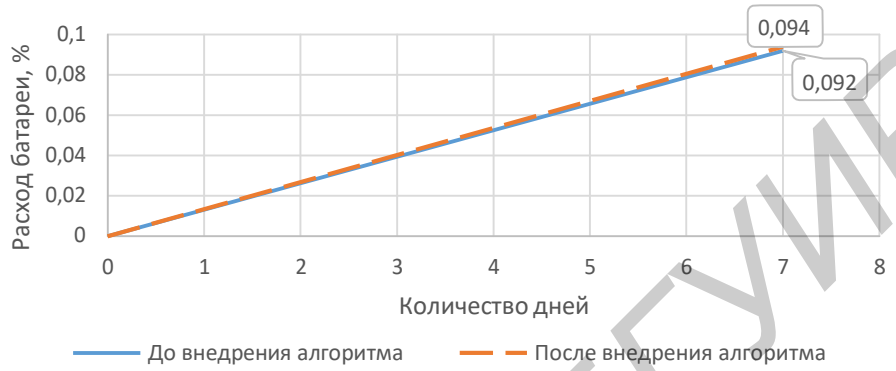

Рисунок 4 – График расхода батареи до внедрения разработанного алгоритма и после внедрения

Техническая реализация разработанного алгоритма подразумевает разработку программного продукта для ОС *Android* на языке программирования *Java*.

Уникальность разработанного алгоритма заключается в использовании комбинированного метода защиты и возможности отправки оповещения пользователю о попытке несанкционированного доступа. Функция отправки данных на электронную почту пользователя является дополнительным уровнем защиты персональных данных и выполняет следующие действия:

– оповещение пользователя;

– своевременное предотвращение утечки персональных данных;

– если мобильное устройство было потеряно или украдено, то геолокация ускорит шансы отыскать его.

В результате *сравнения с альтернативным методом* защиты персональных данных показал свои преимущества: скорость идентификации выше, вероятность успешной идентификации больше в 2 раза и высокий уровень надёжности.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Выполнен обзор различных способов хранения информации на мобильных устройствах. Проведено исследование рынка мобильных приложений, требующих персональных данных пользователя. Систематизированы ос-

новные методы обеспечения безопасности персональных данных пользователей мобильных приложений. Таковыми являются пара «Логин/Пароль», *PIN*-код, графический ключ, одноразовый *SMS*-код, биометрические методы (отпечаток пальца, распознавание по лицу, распознавание по голосу, по подписи).

2. Проведён анализ методов защиты персональных данных и на его основе разработан алгоритм. Согласно которому наиболее популярными и надёжными являются пара «Логин/Пароль» и сканирование отпечатка пальца. На основе этого разработан алгоритм защиты персональных данных пользователей мобильных приложений. Алгоритм состоит из комбинированного способа защиты. Принцип работы такого способа базируется на основе отдельных (стандартных и биометрических) методов. Комбинированный способ включает в себя минимум 2 способа защиты с возможностью выбора одного из них и возможностью простого переключения между ними. В разработанном алгоритме реализовано как раз 2 способа, так как большее количество усложнит интуитивное понимание функционала для пользователя и потребует дополнительных ресурсов при разработке программного представления алгоритма. Также алгоритм включает функцию оповещения пользователя по электронной почте о неудачных попытках идентификации в приложении.

3. Выполнено сравнение альтернативного алгоритма защиты персональных данных, состоящего из последовательных методов: идентификация через «Логин/Пароль», а затем по одноразовому *SMS*-коду.

4. Выполнен анализ разработанного алгоритма по различным критериям и в сравнение с различными способами защита как отдельными, так и комбинированными. В результате анализа использование комбинированного способа защиты персональных данных в разработанном алгоритме является наиболее эффективным, надёжным, простым и быстрым в использовании. Надёжность при использовании отпечатка пальца достигает до 98%, а скорость 1,6 секунды. При необходимости переключения с одного способа на другой, что подразумевает комбинированный метод, общее время идентификации составит 30,4 секунды, что тоже быстрее при различных комбинациях из других методов.

Рекомендации по практическому использованию результатов

1. Применение разработанного алгоритма защиты персональных данных пользователей мобильных устройств возможно при разработке программ для смартфонов и планшетов, поддерживающих операционную систему *Android* с прошивкой 6+. Программа может быть реализована на любом языке программирования, так как алгоритм не привязан к конкретному языку.

2. Разработанный алгоритм является кроссплатформенным. Его можно взять за основу при разработке программ для других операционных систем,

например, *iOS*, и при необходимости доработать его в соответствии с требованиями выбранной ОС.

3. Проведённый обзор различных методов защиты персональных данных пользователей мобильных устройств, анализ их характеристик и взаимодействия друг с другом можно использовать в дальнейших разработках новых способов защиты и модернизации существующих.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Новик, А.М. Использование одноразового *SMS*-кода для аутентификации пользователя на платформе *Android* / А.М. Новик // Электронные системы и технологии: 56-я научная конференция аспирантов, магистрантов и студентов, Минск, 18 – 20 мая 2020 г.: сборник тезисов докладов / Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГУИР, 2020. – С. 364.

2. Новик, А.М. Использование сканера отпечатка пальца для аутентификации пользователя на мобильном устройстве / А.М. Новик // Электронные системы и технологии: 56-я научная конференция аспирантов, магистрантов и студентов, Минск, 2020 г.: сборник тезисов докладов / Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГУИР, 18 – 20 мая 2020. – С. 365.

3. Новик, А.М. Обеспечение безопасности персональных данных пользователей мобильных устройств / А.М. Новик // Электронные системы и технологии: 56-я научная конференция аспирантов, магистрантов и студентов, Минск, 2020 г.: сборник тезисов докладов / Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГУИР, 18 – 20 мая 2020. – С. 366.

4. Новик, А.М. Исследование скорости идентификации пользователя в мобильном приложении различных методов защиты персональных данных / А.М. Новик // Электронные системы и технологии: 57-я научная конференция аспирантов, магистрантов и студентов, Минск, 19 – 23 апреля 2021 г.: сборник тезисов докладов / Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГУИР, 2021. – С. 227.

5. Новик, А.М. Анализ методов защиты персональных данных с точки зрения защищённости процесса идентификации пользователя в мобильном приложении / А.М. Новик // Электронные системы и технологии: 57-я научная конференция аспирантов, магистрантов и студентов, Минск, 19 – 23 апреля 2021 г.: сборник тезисов докладов / Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГУИР, 2021. – С. 224.

РЭЗЮМЭ

Новік Ганна Міхайлаўна

Забеспячэнне бяспекі дадзеных карыстальнікаў мабільных прылад

Ключавыя словы: персанальныя дадзеныя, мабільнае прыкладанне, алгарытм, праграмны модуль.

Мэта працы: распрацоўка алгарытму абароны персанальных дадзеных карыстальнікаў мабільных прыкладанняў з далейшым укараненнем у праграмны модуль, тэставаннем тэхнічнай часткі і поўным аналізам гатовага алгарытму.

Атрыманыя вынікі і іх навізна: прааналізаваныя метады абароны персанальных дадзеных карыстальнікаў і мабільныя прыкладання, якія выкарыстоўваюць гэтыя дадзеныя. Распрацаваны алгарытм абароны персанальных дадзеных, які з'яўляецца кросплатформенным і складаецца з камбінаванага спосабу абароны («Лагін/Пароль» і біяметрычны: сканер адбітка пальца) і мае функцыю аўтаматычнай адпраўкі паведамлення карыстачу на электронную пошту ў выпадку няправільнай спробы ідэнтыфікацыі. Прапанаваная магчымая рэалізацыя распрацаванага алгарытму ў праграмным модулі для аперацыйнай сістэмы *Android* на мове праграмавання *Java*. Згодна з праведзенага аналізу распрацаванага алгарытму, ідэнтыфікацыя карыстальніка з дапамогай адбітка пальца з'яўляецца найбольш хуткай з усіх (~1,6 секунды), цяжка падраблялі і, адпаведна, больш надзейнай (~97% захаванасці персанальных дадзеных) сярод астатніх разгледжаных метадаў.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі» у навучальны курс «Сучасныя тэхналогіі праектавання інфармацыйных сістэм».

Вобласць ужывання: мабільныя тэхналогіі, камп'ютэрная бяспека, распрацоўка мабільных прыкладанняў.

РЕЗЮМЕ

Новик Анна Михайловна

Обеспечение безопасности данных пользователей мобильных устройств

Ключевые слова: персональные данные, мобильное приложение, алгоритм, программный модуль.

Цель работы: разработка алгоритма защиты персональных данных пользователей мобильных приложений с дальнейшим внедрением в программный модуль, тестированием технической части и полным анализом готового алгоритма.

Полученные результаты и их новизна: проанализированы методы защиты персональных данных пользователей и мобильные приложения, использующие эти данные. Разработан алгоритм защиты персональных данных, который является кроссплатформенным и состоит из комбинированного способа защиты («Логин/Пароль» и биометрический: сканер отпечатка пальца) и имеет функцию автоматической отправки сообщения пользователю на электронную почту в случае неверной попытки идентификации. Предложена возможная реализация разработанного алгоритма в программном модуле для операционной системы *Android* на языке программирования *Java*. Согласно проведённому анализу разработанного алгоритма, идентификация пользователя с помощью отпечатка пальца является наиболее быстрой из всех (~1,6 секунды), трудно подделываемой и, соответственно, более надежной (~97% сохранности персональных данных) среди остальных рассмотренных методов.

Степень использования: результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Современные технологии проектирования информационных систем».

Область применения: мобильные технологии, компьютерная безопасность, разработка мобильных приложений.

SUMMARY
Novik Hanna Mikhailovna
Ensuring the security of data of users of mobile devices

Keywords: personal data, mobile application, algorithm, software module.

Purpose of work: development of an algorithm for protecting personal data of users of mobile applications with further implementation into the software module, testing the technical part and a complete analysis of the finished algorithm.

The results and novelty: methods of protecting personal data of users and mobile applications using this data have been analyzed. A personal data protection algorithm has been developed, which is cross-platform and consists of a combined protection method ("Login/Password" and biometric: fingerprint scanner) and has the function of automatically sending a message to the user by e-mail in case of an incorrect identification attempt. A possible implementation of the developed algorithm in a software module for the Android operating system in the Java programming language is proposed. According to the analysis of the developed algorithm, user identification using a fingerprint is the fastest of all (~1.6 seconds), difficult to counterfeit and, accordingly, more reliable (~97% of personal data safety) among the other methods considered.

Degree of use: the results were introduced into the educational process at the department of design of information and computer systems of the educational institution "Belarusian State University of Informatics and Radioelectronics" in the training course "Modern technologies for the design of information systems."

Sphere of application: mobile technology, computer security, mobile application development.