

Государственное образовательное учреждение
высшего профессионального образования
“ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ”
Физико-технический факультет
Кафедра радиофизики и инфокоммуникационных технологий
Направление подготовки 10.04.01 Информационная безопасность

Магистерская диссертация на тему:
**Защита данных в мобильных приложениях для
систем ограничения доступа**

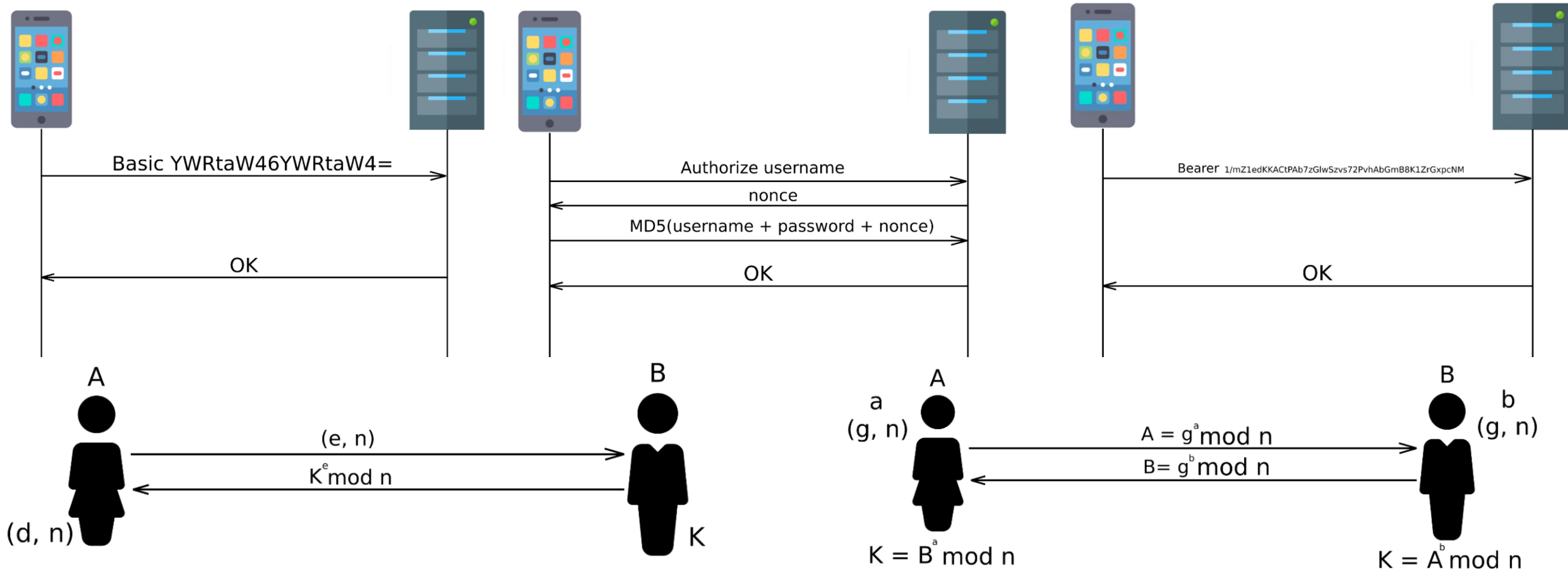
Студент: Поздняков Александр Андреевич
Научный руководитель: к. ф-м. н. доцент Безус А. В.
ст. преподаватель Бабичева М.В.

- **Цель работы** - анализ уязвимостей мобильных приложений под управлением операционной системы Android
- **Объект исследования** - мобильные приложения для систем ограничения доступа под Android
- **Предмет исследования** - уязвимости клиентской и серверной части мобильных приложений под управлением операционной системы Android
- **Научная новизна** - разработан и внедрен алгоритм установления безопасного канала передачи данных между клиентом и сервером; создана расширенная классификация разрешений приложений в системе Android и разработан метод анализа опасности приложений на основе новой классификации.

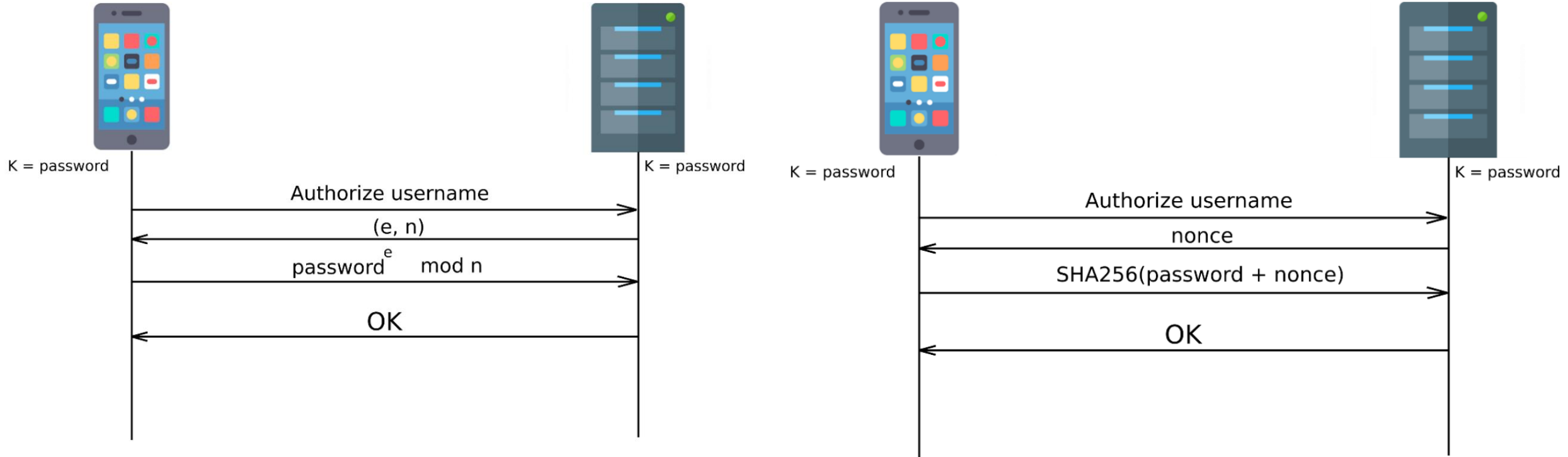
Постановка задачи:

- разработать и внедрить мобильное приложение для обмена данными по защищенному каналу в системе ограничения доступа на объект;
- разработать приложение имитирующее инструмент удаленного доступа для проведения тестовых экспериментов;
- провести эксперименты по реализации атак на мобильное приложение и мобильные устройства различных типов;
- обобщить результаты экспериментов и предложить методику защиты от подобного рода атак.

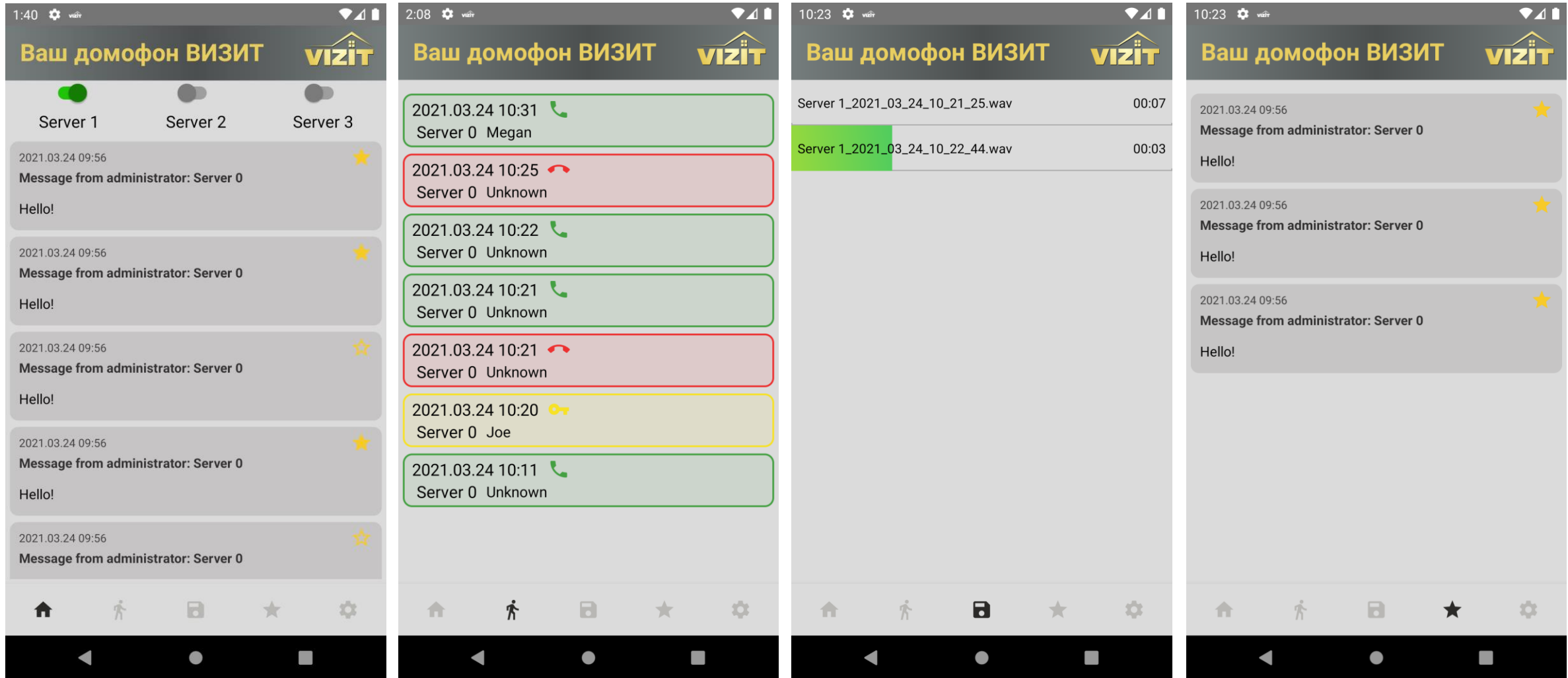
Анализ известных схем аутентификации и создания защищенного канала передачи данных

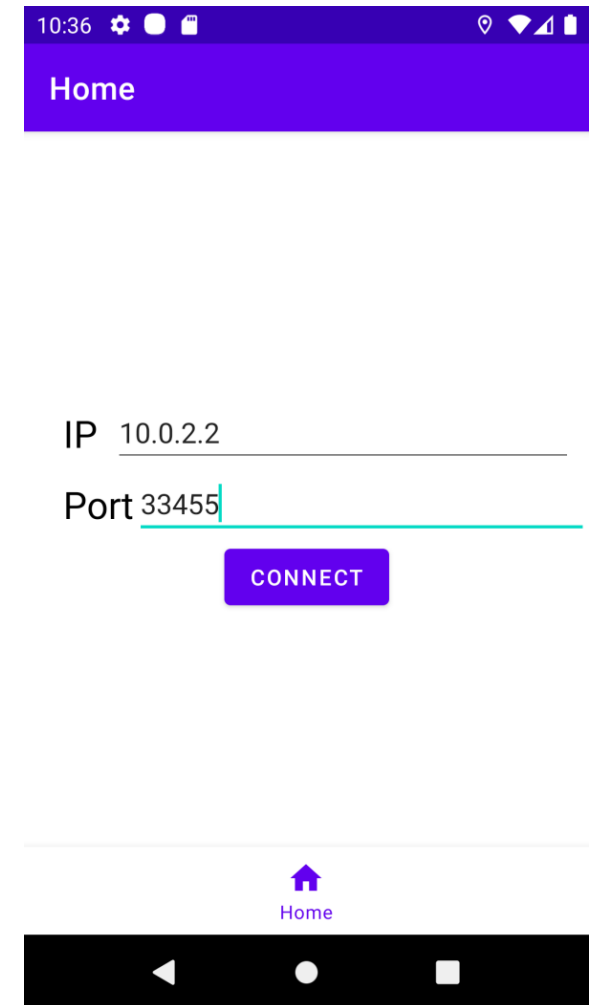


Разработка алгоритма аутентификации с созданием безопасного канала передачи данных



Создание приложения для системы ограничения доступа

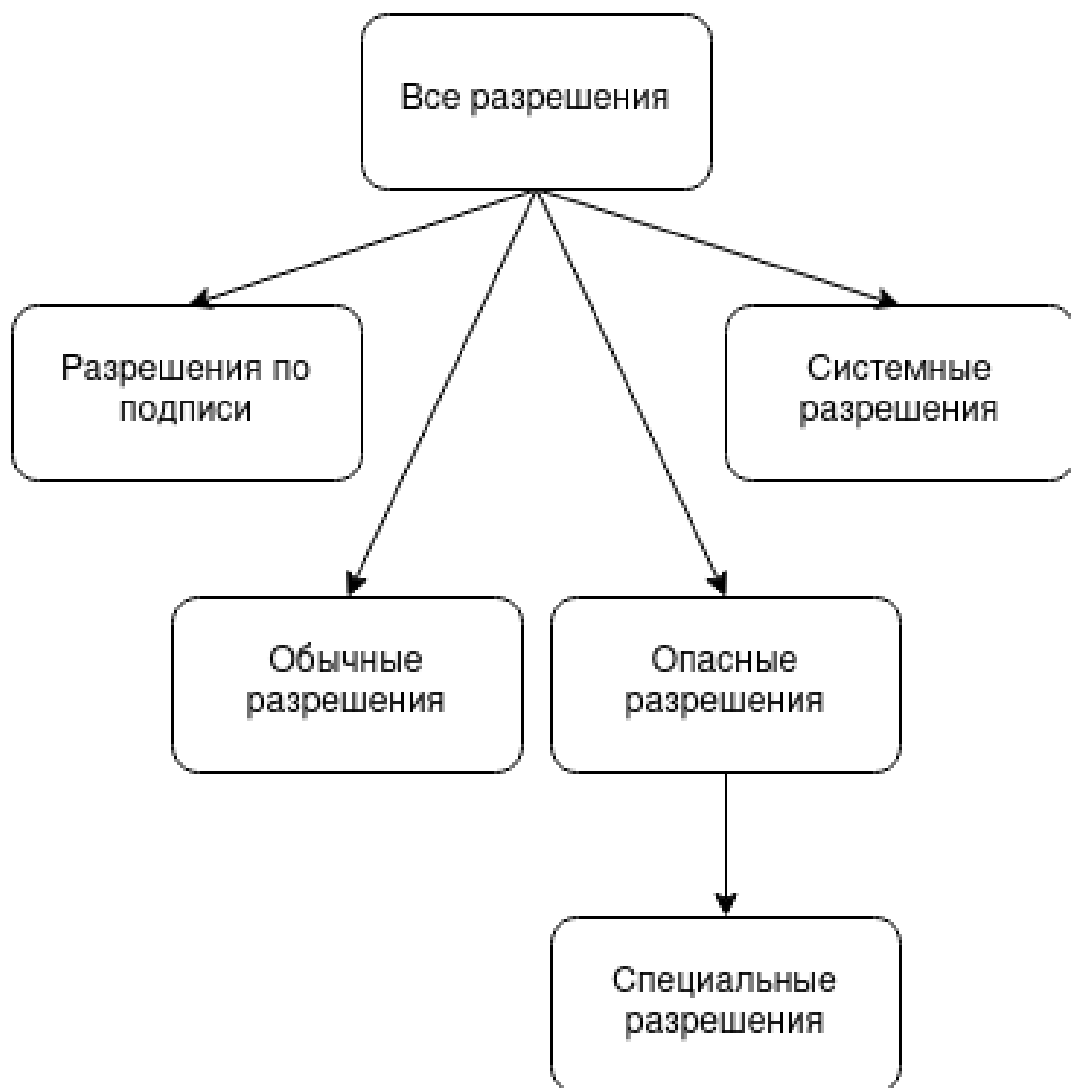




Результаты экспериментов

		Версия Android						
		5	6	7	8	9	10	11
Команда	Информация об устройстве	+	+	+	+/-	+/-	+/-	+
	Контакты	+	+	+	+	+	+	+/-
	Местоположение	+	+	+	+	+	+	+
	Сообщения	+	+	+	+	+	+	+

Классификация опасности разрешений



Класс	Диапазон коэффициентов	Описание
Неопасные	0 - 10	Разрешения, позволяющие приложению собирать минимальное количество информации, или не позволяющее собирать информацию вовсе.
Опасные	11 - 14	Разрешения, позволяющие собирать конфиденциальную информацию о пользователе, сбор которой даёт злоумышленникам ограниченный набор возможностей.
Критические	15 - 20	Разрешения, позволяющие собирать критически важную информацию, дающую злоумышленникам большие возможности для проведения последующих атак.

Математическая модель анализа приложений

$$K_1 = \sum_i p_i$$

$$K_2 = \alpha C + \beta D + \gamma N$$

$$S = \begin{cases} 0, & K_2 < p_1 \\ 1, & p_1 \leq K_2 < p_2 \\ 2, & p_2 \leq K_2 \end{cases}$$

Проведение экспериментов и корректировка коэффициентов

MTS Phoenix 11:00 AM

PermissionsChecker

Viber	180
Telegram	133
Альфа-Банк	107
VK	107
Duolingo	64
Домофон	59
Yandex.Maps	56
Office	54
Firefox	53
ЦРБ Онлайн	44
Yandex.Mail	43
Robot36	43
weawow	40
Firefox Focus	35

Navigation bar: back, home, recent apps

$$\alpha = 3, \beta = 0.75, \gamma = 0.05$$

$$p_1 = 6 \quad p_2 = 4$$

MTS Phoenix 1:52 PM

PermissionsChecker

Viber	180
Telegram	133
Альфа-Банк	107
VK	107
RAT	96
Duolingo	64
Домофон	59
Yandex.Maps	56
Office	54
Firefox	53
ЦРБ Онлайн	44
Yandex.Mail	43
Robot36	43
weawow	40

Navigation bar: back, home, recent apps

$$\alpha = 1.35, \beta = 0.25, \gamma = 0.075$$

$$p_1 = 5.5 \quad p_2 = 3$$

Анализ других шпионских программ

PermissionsChecker	
System Framework	319
Backup	305
Device Health	287
RAT	115
Домофон	66
Kids	54
Persona	50
PermissionsChecker	0

PermissionsChecker	
Viber	
com.viber.voip	
180	
android.permission.RECORD_AUDIO	20
Allows an application to record audio.	
android.permission.READ_CONTACTS	19
Allows an application to read the user's contacts data.	
android.permission.READ_PHONE_STATE	17
Allows read only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.	
android.permission.ACCESS_FINE_LOCATION	16
Allows an app to access precise location.	
android.permission.CAMERA	14
Required to be able to access the camera device. Allows application to take photos and videos	
android.permission.ACCESS_COARSE_LOCATION	14
Allows an app to access approximate location	

ВЫВОДЫ

В ходе данной работы были созданы три различных мобильных приложения, каждое из которых использовалось для исследования безопасности мобильных приложений для операционной системы Android, а также самой операционной системы.

С помощью написанного приложения для тестирования уровня защиты операционной системы Android от шпионского программного обеспечения удалось беспрепятственно собирать конфиденциальные пользовательские данные. Это показало, что операционная система Android не обладает фактически никакой защитой от шпионских приложений. Выявлением и блокировкой таких приложений вынуждены заниматься сами пользователи.

Написанный на основе предложенной математической модели анализа приложений автоматический анализатор позволил с большой точностью выявлять потенциально опасные приложения.

Разработанный алгоритм аутентификации с установлением безопасного канала связи был внедрён на предприятии ФИРМА “МДЛ” при разработке нового программного обеспечения.

Предварительные результаты работы были опубликованы в статье “Алгоритм аутентификации пользователя с созданием безопасного канала передачи данных в коммуникационных системах на основе протокола UDP” в журнале “Вестник Донецкого национального университета”, серия Г, технические науки, 2020, номер 4, стр. 12.

СПАСИБО ЗА ВНИМАНИЕ!