Информационная безопасность Android

Лекция 4.1

Kotlin

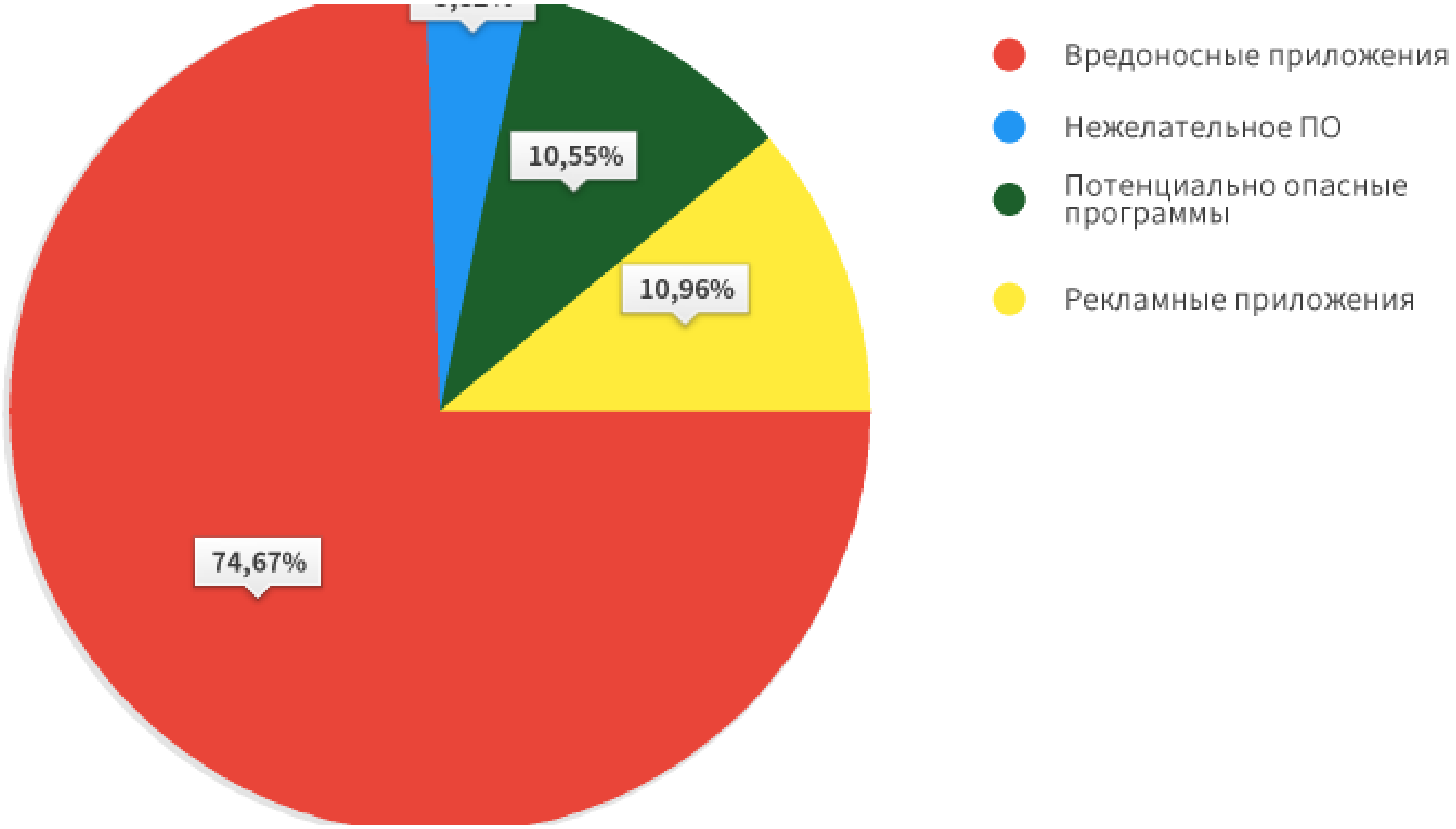
Ключев А.О. к.т.н., доцент ФПИиКТ Университета ИТМО

Санкт-Петербург

2025

Литература и полезные ссылки

- «Доктор Веб»: обзор вирусной активности для мобильных устройств за 2024 год
- Мобильная вирусология 2024 (Kaspersky)
- Типы ошибок связанных с инф. безопасностью в Android (Google)
- Классификация вредоносного ПО в Android (Google)
- Развитие механизмов безопасности Android (от версии к версии)
- Что нового в безопасности пользователей на Android: доклад с Google I/O 2024
- Почему антивирусы под Android бесполезны, и что с этим делать (2015)
- **Нужен ли антивирус для Android в 2023 году?**


10,55%
10,96%
74,67%
Вредоносные приложения
Нежелательное ПО
Потенциально опасные программы
Рекламные приложения

Механизмы информационной безопасности Android

- **Песочница (Sandbox)**: каждое приложение работает в изолированной среде, не имея доступа к данным других приложений без разрешения.
- **Система разрешений**: пользователь или система решает, к чему приложение может получить доступ (камера, контакты, файлы и т.д.).
- **Google Play Protect**: встроенный инструмент сканирует приложения в магазине и на устройстве на наличие вредоносного кода.

Как заразить систему на базе Android

- **Установка приложений из сторонних источников**: APK-файлы, скачанные не из Google Play, могут содержать вредоносный код. Например, трояны маскируются под легитимные приложения (игры, утилиты).
- **Фишинг**: пользователь переходит по ссылке, скачивает файл или вводит данные на поддельном сайте, что приводит к установке вредоносной программы.
- **Эксплуатация уязвимостей**: если система или приложение не обновлены, хакеры могут использовать известные баги (например, в WebView или ядре Linux).
- **Социальная инженерия**: пользователь сам дает разрешения вредоносному приложению, не осознавая последствий.

Защита

Для пользователей:

- Установка приложения только из официальных магазинов приложений (например, из Google Play, если он есть).
- Проверка разрешений приложений перед установкой.
- Не переходить по подозрительным ссылкам.
- Регулярно обновлять систему и приложения (обычно обновления безопасности выходят несколько лет)

Для разработчиков:

- Использование безопасных API и библиотек.
- Шифрование данных (например, с помощью Jetpack Security).
- Проверка вводимых данных для защиты от инъекций.

О пользе антивирусов

Аргументы "за":

- Антивирусы (например, Avast, Kaspersky, Bitdefender) могут обнаруживать вредоносные APK, фишинговые ссылки и подозрительное поведение приложений.
- Они полезны, если вы часто устанавливаете приложения из сторонних источников или не обновляете устройство.
- Некоторые антивирусы предлагают дополнительные функции: защита от кражи, VPN, очистка памяти.

Аргументы "против":

- Google Play Protect уже встроен в Android и обновляется автоматически. Он покрывает базовые угрозы (к сожалению, часть программ приходится ставить из других магазинов приложений)
- Антивирусы могут замедлять устройство и потреблять ресурсы.
- Многие **бесплатные** антивирусы сами собирают данные пользователей, что снижает их полезность с точки зрения приватности.

Старые версии Android

- На март 2025 года около 30% устройств работают на Android 11 или ниже (по данным StatCounter).
- Google прекращает поддержку старых версий через 3–4 года после релиза. Например, Android 9 (Pie) уже не получает обновлений безопасности с 2022 года.
- Производители устройств часто не обновляют прошивки после 2–3 лет, даже если Google выпускает патчи. Обычно чем дешевле устройство, тем меньше обновлений.

Риски использования старых версий Android

1. **Уязвимости**: Старые версии содержат известные баги, которые хакеры могут эксплуатировать. Например, уязвимость Stagefright (2015) до сих пор актуальна для необновленных устройств.
2. **Отсутствие новых функций безопасности**: Android 12 и выше ввели улучшенные механизмы контроля разрешений и изоляции данных, которых нет в старых версиях.
3. **Несовместимость** с приложениями: современные приложения могут не работать на устаревших системах, вынуждая пользователей искать небезопасные альтернативы.

Банковские трояны

- Как работают: Маскируются под легитимные приложения, крадут данные банковских карт или перехватывают SMS с кодами подтверждения.
- Пример: FluBot, распространяемый через фишинговые SMS.
- Защита: Не скачивайте приложения по ссылкам из SMS, используйте двухфакторную аутентификацию (2FA).

Программы-вымогатели (Ransomware)

- Как работают: Шифруют файлы на устройстве и требуют выкуп.
- Пример: Lockerpin, блокирующий экран.
- Защита: Регулярно делайте резервные копии, не устанавливайте подозрительные APK.

Zero Day - уязвимость нулевого дня

- **Уязвимость zero-day** (или "уязвимость нулевого дня") — это ошибка или слабое место в программном обеспечении, о котором разработчики еще не знают или не успели выпустить исправление. Название "zero-day" отражает тот факт, что у разработчиков есть ноль дней на подготовку защиты после того, как уязвимость становится известной злоумышленникам.
- **Обнаружение**: Хакеры или исследователи находят уязвимость раньше, чем разработчики ПО (например, Google для Android).
- **Эксплуатация**: Злоумышленники создают код (эксплойт), который использует эту уязвимость для атаки — например, для получения доступа к системе, кражи данных или установки вредоносного ПО.
- **Отсутствие защиты**: Поскольку патча еще нет, стандартные меры безопасности (антивирусы, обновления) не помогают.

Атаки через уязвимости zero-day

- Как работают: Используют неизвестные баги в системе или приложениях.
- Пример: Уязвимости в чипах Qualcomm (2024) позволяли удаленно выполнять код.
- Защита (ее почти нет):
  - Чаще обновляйте систему,
  - Не ставьте APK из подозрительных мест (антивирус скорее всего ничего не найдет!)
  - Избегайте root-доступа.
  - Не используйте небезопасные библиотеки
  - Тестируйте код на уязвимости
  - Анализируйте нетипичное поведение программ, странный сетевой трафик, обращение к устройствам и т.п.

Фишинг и поддельные приложения

- Как работают: Пользователя обманом заставляют установить приложение или ввести данные.
- Пример: Поддельные версии WhatsApp с рекламой или шпионским ПО.
- Защита: Проверяйте разработчика в Google Play, используйте антифишинговые браузеры.

Для разработчиков

- Используйте ProGuard или R8 для обфускации кода.
- Применяйте подпись приложений (App Signing) через Google Play.
- Тестируйте приложения на уязвимости с помощью инструментов вроде OWASP Mobile Security Testing Guide.

Зачем нужен вредоносный код?

- Для хакеров:
  - Кража средств с банковских счетов
  - Кража личных данных, слежка за людьми
  - Реклама
  - Рассылка спама
  - Ботнеты (DDOS атаки, взлом и т.п.)
  - Майнинг криптовалют
- Ну и похоже, что бурная деятельность по взлому поддерживает необходимость постоянного обновления софта и железа для пользователей =)

Спасибо за внимание!