

ANTI-SPYWARE DASTURLARINING AHAMIYATI VA ANDROID OS- DA XAVFSIZLIKNI TA'MINLASHDAGI ROLI

*Muhammad al-Xorazmiy nomidagi
Toshkent Axborot Texnologiyalari universiteti
Farg'ona filiali Abdurashidov Saydullo*

*Mobil qurilmalar inson hayotining ajralmas qismiga aylandi. Android OS, ochiq kodli bo'lishi sababli, eng keng tarqalgan operatsion tizim hisoblanadi. Shu bilan birga, uning ochiq ekotizimi turli xavf-xatarlarga, xususan **spyware** (josus dasturlar) kabi zararli dasturlarga duchor qiladi. **Spyware** foydalanuvchi ruxsatisiz ma'lumotlarni kuzatish, to'plash va tarqatish uchun ishlatiladi. Bu muammo Android foydalanuvchilari uchun jiddiy xavf tug'diradi. Shu sababli, **anti-spyware dasturlarining ahamiyati** katta bo'lib, ular qurilma xavfsizligini ta'minlashda muhim rol o'ynaydi.*

***Tayanch iboralar:** Spyware, Anti-Spyware dasturlari, Android OS, Zararli dasturlar, Ilova ruxsatnomalari, Real vaqt monitoringi, Shaxsiy ma'lumotlar himoyasi, Google Play Store, Mobil xavfsizlik.*

Мобильные устройства стали неотъемлемой частью жизни людей. Android является самой распространенной операционной системой, поскольку она является открытой. В то же время, его открытая экосистема подвержена различным угрозам, в частности вредоносным программам, таким как шпионское программное обеспечение. Шпионское ПО используется для наблюдения, сбора и распространения данных без согласия пользователя. Эта проблема представляет серьезную угрозу для пользователей Android. Поэтому антишпионские программы играют важную роль в обеспечении безопасности устройств.

***Ключевые слова:** Spyware, Анти-шпионские программы, ОС Android, Вредоносное ПО, Разрешения приложений, Мониторинг в реальном*

времени, Защита персональных данных, Google Play Store, Мобильная безопасность.

Mobile devices have become an integral part of human life. Android OS is the most popular operating system because it is open source. However, its open ecosystem is vulnerable to various threats, most notably malware such as spyware. Spyware is used to monitor, collect, and distribute data without user consent. This problem poses a serious threat to Android users. This is why anti-spyware software is so important, and why it plays such an important role in ensuring device security.

Keywords: *Spyware, Anti-spyware, Android OS, Malware, Application Permissions, Real-time monitoring, Privacy Protection, Google Play Store, Mobile Security.*

Kirish

Bugungi kunda mobil qurilmalar inson hayotining ajralmas qismiga aylangan bo‘lib, ularda saqlanadigan shaxsiy va xizmat ma’lumotlari himoyasini ta’minlash muhim ahamiyatga ega. Android operatsion tizimi dunyoning eng keng tarqalgan va ochiq kodli platformasi hisoblanadi, shu sababli u ham ishonchli foydalanuvchilar, ham kiberhujumchilar e’tiborida bo‘ladi. Shunday ekan, Android qurilmalarining kiberxavfsizligini ta’minlashda ilg‘or texnologiyalar va anti-spyware dasturlardan foydalanish muhimdir.

Spyware (josus dasturlar) orqali shaxsiy ma’lumotlarni ruxsatsiz kuzatish va o‘g‘irlash holatlari tobora ko‘paymoqda. Bunday sharoitda, anti-spyware dasturlari mobil qurilmalarni himoya qilish uchun ishonchli vositalar sifatida xizmat qiladi. Ularning roli ma’lumotlar xavfsizligini ta’minlash, shubhali faoliyatlarni aniqlash va zararli dasturlarni zararsizlantirishda katta ahamiyat kasb etadi.

Ushbu maqolada **anti-spyware dasturlarining** ahamiyati, ularning Android operatsion tizimida xavfsizlikni ta’minlashdagi roli va ularning foydalanish samaradorligi tahlil qilinadi.

Asosiy qism

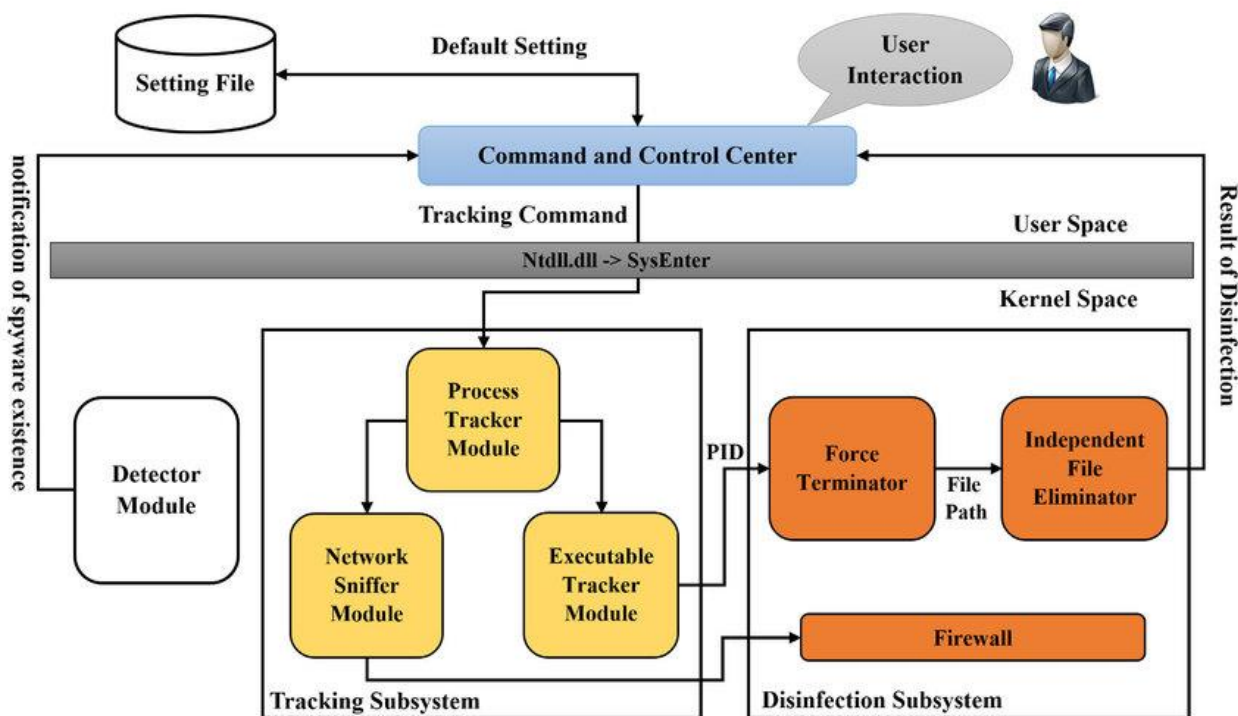
Spyware — bu foydalanuvchi ruxsatisiz shaxsiy ma'lumotlarni yig'adigan zararli dasturlar turidir. Ushbu dasturlar odatda qurilmaga uchinchi tomon ilovalari, phishing hujumlari yoki zararli havolalar orqali kiradi. Spyware foydalanuvchining joylashuvini kuzatishi, bank ma'lumotlari va parollarni o'g'irlashi, qurilma kamerasidan yashirincha foydalanishi, shuningdek, matnli xabarlar va qo'ng'iroqlarni kuzatishi mumkin. Bunday faoliyat foydalanuvchining shaxsiy hayotiga zarar yetkazib, moliyaviy xavfsizlikka tahdid soladi. Shu sababli, spyware tahdidlarini oldini olish va zararsizlantirish muhim hisoblanadi. Android operatsion tizimi dunyoning eng keng tarqalgan va ochiq kodli platformasi hisoblanadi. Biroq, uning ochiq kodli bo'lishi rivojlanishni osonlashtirgani bilan birga, zararli dasturlar uchun keng imkoniyatlar yaratadi. Android xavfsizligidagi muammoli jihatlar orasida ilova ruxsatnomalari, rootlash xavflari va zararli ilovalarning mavjudligi alohida e'tiborga loyiqdir. Ko'pgina ilovalar foydalanuvchilardan ortiqcha ruxsatlar talab qiladi, bu esa shaxsiy ma'lumotlarning noqonuniy foydalanilishiga olib kelishi mumkin. Qurilmalarni rootlash orqali foydalanuvchilar tizim cheklovlarini olib tashlaydi, ammo bu zararli dasturlar uchun kirish imkonini oshiradi. Shuningdek, Google Play Store'da ham ba'zan zararli ilovalar uchrab turadi, bu esa foydalanuvchilar uchun qo'shimcha xavf tug'diradi.

Anti-spyware dasturlari Android qurilmalarining xavfsizligini ta'minlashda muhim ahamiyatga ega. Ushbu dasturlar josuslik dasturlarini aniqlash va o'chirish, foydalanuvchining shaxsiy va moliyaviy ma'lumotlarini himoya qilish, shubhali faoliyatlarni aniqlash kabi funksiyalarni bajaradi. Bundan tashqari, anti-spyware dasturlar qulay interfeysga ega bo'lib, foydalanuvchilar uchun foydalanishni osonlashtiradi. Bunday dasturlar real vaqt rejimida zararli faoliyatlarni kuzatib, foydalanuvchining xavfsizligini ta'minlaydi. Spyware tahdidlarini minimallashtirish uchun foydalanuvchilar va ishlab chiquvchilar faqat ishonchli manbalardan ilovalarni yuklab olish, ilova ruxsatnomalarini muntazam ravishda ko'rib chiqish, qurilmada antivirus yoki anti-spyware

dasturlarini oʻrnatish, shuningdek, dasturiy taʼminot yangilanishlarini oʻz vaqtida amalga oshirish kabi choralarni koʻrishi lozim.

Soʻnggi yillarda anti-spyware dasturlarida sunʼiy intellekt texnologiyalarining joriy etilishi josuslik dasturlarini oldindan bashorat qilish va ularni bloklash imkonini yaratdi. Shuningdek, real vaqt monitoringi texnologiyalari qurilmadagi barcha harakatlarni kuzatib, xavfsizlikni yanada oshirdi. Maʼlumotlarni shifrlash texnologiyalari esa foydalanuvchining shaxsiy maʼlumotlarini himoya qilib, begona kirishni chekladi. Android OS uchun anti-spyware dasturlari kiberxavfsizlikni taʼminlashda asosiy vositalardan biri boʻlib, mobil qurilmalarni josuslik dasturlari tahdididan himoya qilishda muhim rol oʻynaydi. Ushbu dasturlar foydalanuvchilarni zararli dasturlardan himoya qilish orqali mobil xavfsizlikning zamonaviy talablarini qondiradi.

Android OS da anti-spyware dasturlarni tuzishda birinchi oʻrinda eʼtibor beriladigan jihat, Android dasturlari uchun beriladigan ruxsatlar, yaʼni permissionlarni tekshirib chiqish lozim. Chunki Android OS da koʻp spyware dasturlari fishing orqali bevosita foydalanuvchilarni oʻzlaridan zarur ruxsatlarni soʻrab olish orqali ularning shaxsiy maʼlumotlarini (parollar, qurilma kamerasi, qurilma diktafoni va qoʻngʻiroqlar tarixi) oʻzlashitirib olishmoqda. Bularni inobatga olgan holatda, Android qurilmadagi barcha dasturlar ruxsatlarini nazorat qiladigan anti-spyware dasturlarini yaratish hozirgi zamonaviy dunyomizning zaruriy talabi boʻlib qolmoqda. Anti-Spyware dasturlari turli xil arxitekturalar asosida quriladi, biz mana shu arxitekturalar orasida keng tarqalganlari bilan tanishamiz. (1-rasm)



Rasm 1. Anti-spyware dasturlarning arxitekturasi

Xulosa

Mobil texnologiyalar hayotimizning ajralmas qismiga aylangan bir davrda, Android operatsion tizimi dunyoning eng keng tarqalgan platformalaridan biri sifatida shaxsiy va xizmat ma'lumotlari xavfsizligini ta'minlash masalasini dolzarb qilib qo'ymoqda. Spyware kabi zararli dasturlar foydalanuvchilarning shaxsiy hayoti va moliyaviy xavfsizligiga jiddiy tahdid soladi. Ushbu tahdidlarga qarshi kurashda anti-spyware dasturlari eng samarali vosita sifatida namoyon bo'lmoqda. Anti-spyware dasturlar Android qurilmalarini josuslik dasturlaridan himoya qilish, shubhali faoliyatlarni aniqlash va foydalanuvchi ma'lumotlarini xavfsiz saqlashda katta ahamiyat kasb etadi. Ular sun'iy intellekt, real vaqt monitoringi va ma'lumotlarni shifrlash kabi ilg'or texnologiyalardan foydalangan holda, kiberxavfsizlikni yangi darajaga olib chiqmoqda. Spyware tahdidlarini minimallashtirish uchun foydalanuvchilar faqat ishonchli manbalardan ilovalarni yuklab olish, ilova ruxsatnomalarini sinchkovlik bilan tekshirish va muntazam ravishda dasturiy ta'minotni yangilab borishlari zarur. Shu bilan birga, ishlab chiquvchilar xavfsizlikni kuchaytirishga qaratilgan zamonaviy texnologiyalarni joriy etishlari lozim.

Xulosa qilib aytganda, Android qurilmalarining xavfsizligini ta'minlashda anti-spyware dasturlar muhim rol o'ynaydi. Foydalanuvchilarning ma'lumotlarini himoya qilish va josuslik dasturlarining salbiy ta'sirini bartaraf etish orqali ular mobil xavfsizlikni ta'minlashda ishonchli vosita hisoblanadi. Shu sababli, foydalanuvchilar kiberxavfsizlikka jiddiy e'tibor qaratib, o'z qurilmalarini himoya qilish choralarini ko'rishlari lozim.

FOYDALANILGAN ADABIYOTLAR:

1. *Muxammadovich, M. F., & Maxammad o'g'li, U. A. (2022, November). AXBOROTNI XIMOYALASH TIZIMINI ISHLAB CHIQISH. In Proceedings of International Educators Conference (Vol. 1, No. 2, pp. 187-190).*
2. *Умаров, А. (2023, November). ИНТЕГРИРОВАННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ В ВУЗАХ: ТЕОРИЯ И ПРАКТИКА. In Conference on Digital Innovation: "Modern Problems and Solutions".*
3. *T. D. H. (2023). CISCO PACKET TRACER YORDAMIDA HUSUSIY KORXONALAR UCHUN MAXSUS HIMOYALANGAN TARMOQ KANALI ISHINI LOYIHALASH. Al-Farg'oniy avlodlari, 1(3), 25-32*
4. *Tojimatov, D. X. (2022). Kiberxavfsizlik: tahdilar; muammolar; yechimlar; "Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar" Respublika Ilmiy-texnik anjumani TATU Farg'ona filiali.*
5. *Umarov, A. (2023, November). Xavfsizlik hodisalari: profilaktika choralari va ma'lumotlardan ruxsatsiz foydalanishga qarshi choralar. In Conference on Digital Innovation: "Modern Problems and Solutions".*
6. *Umarov, A. (2023, November). Axborotni ichki tahdidlardan himoya qilish: ruxsatsiz foydalanishning oldini olish. In Conference on Digital Innovation: "Modern Problems and Solutions".*
7. *Тождматов, Д. (2023, October). ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ. In Conference on Digital Innovation: "Modern Problems and Solutions". Umarov, A.*

M. O. G. L. (2021). AXBOROT XAVFSIZLIGI XAVFINI BAHOLASH. Scientific progress, 2(8), 293-300.

8. Тоџиматов, Д. (2023, November). ПРИМЕНЕНИЕ ИНТЕРАКТИВНЫХ МЕТОДОВ В ПРЕПОДАВАНИИ КРИПТОГРАФИИ: РАЗВИТИЕ АНАЛИТИЧЕСКИХ И РЕШАЮЩИХ ПРОБЛЕМ НАВЫКОВ. In Conference on Digital Innovation: "Modern Problems and Solutions". Мухаммадович, М. F., & Махаммад о'г'ли, У. А. Ro'zaliyev Abdumalikjon Vahobjon о'г'ли. (2022). AXBOROTNI XIMOYALASH.