Оқытушы: Кинтонова А.Ж.

Компьютерлік ақпараттарды қорғаудың технологиялары

**№ 9 практикалық жұмыс:** Android –та сүзгілеуді орнату әдістері.

**Мақсаты:** Android -та сүзгілеуді орнату әдістерін зерттеп, пайдалану.

 **Практикалық тапсырма:** Android – та сүзгілеуді орнату әдістерін зерттеп, пайдалану. Android телефонында құпиялылықты қорғау әдістерін пайдаланып орындаңыз. Есеп жасаңыз. Скриншоттарға түсініктемелерін жазыңыз.

**Әдебиет:**

[ТОП-5 способов защитить Android (встроенными средствами) - YouTube](https://www.youtube.com/watch?v=wgjOz1LK2kQ)

[Лучшая программа для защиты личных данных на телефоне! - YouTube](https://www.youtube.com/watch?v=BgWJFI6cI7Y&t=292s)

[СРОЧНО ОТКЛЮЧИ ЭТИ НАСТРОЙКИ НА СВОЕМ СМАРТФОНЕ! ХИТРОСТЬ РАЗРАБОТЧИКОВ ПРО СБОР ЛИЧНЫХ ДАННЫХ - YouTube](https://www.youtube.com/watch?v=kisJQhs9Oxg)

[1815.pdf (ifmo.ru)](https://books.ifmo.ru/file/pdf/1815.pdf) - Учебное пособие «Программирование под платформу Android»

[Создание средства антивирусной защиты для ОС Android (refleader.ru)](http://refleader.ru/merotrujgujg.html)

 [Лучшая программа для защиты личных данных на телефоне! - YouTube](https://www.youtube.com/watch?v=BgWJFI6cI7Y)

[Родительский контроль на Android - YouTube](https://www.youtube.com/watch?v=Q5eGOqOLTVM&t=179s)

[Родительский контроль на андроид в 2021. как установить сделать родительский контроль на Телефоне - YouTube](https://www.youtube.com/watch?v=vc5aS6sMNbo)

[Защита личных данных на Android-телефоне / Хабр (habr.com)](https://habr.com/ru/post/379107/)

**Теориялық бөлімі.**

* Ұялы компьютерлер ұзақ уақыт бойы стационарлық компьютерлерден басым болды. Стационарлық мәліметтерге қарағанда, оларда біздің жеке деректеріміз әлдеқайда көп. Сонымен қатар, мобильді құрылғылардың ОЖ-нің қазіргі дизайны олардың негізгі міндеттерінің бірі - үшінші тараптарға (негізінен корпорациялар мен мемлекетке) қол жетімділікті мүмкіндігінше жеңілдету деген әсер қалдырады, бірақ мобильді қосымшалардың шағын жасаушылары да бұзылады осы пирогтан) сіздің жеке деректеріңізге. Android ішінара ашықтығы жағдайды сәл жақсартады, бірақ жеке деректердің ағып кетуіне қатысты толыққанды шешім әлі жоқ. Басты мәселе, құрылғыда блоктар қолданылып жатқанда, оларда бетбелгілер жоқ екеніне кепілдік жоқ (Samsung Galaxy микробағдарламасында табылған сияқты). Ашық көзі жоқ меншікті қосымшалармен ұқсас проблема (Google Play дүкенінің өзінен бастап бүкіл GApps пакеті сияқты). Шын мәнінде, бәрі керісінше - ол жерде бетбелгілер болуы әбден мүмкін. Көбіне олар оларды жасыруға тырыспайды, синхрондау және / немесе сақтық көшірме жасау, сізге пайдалы жарнама ұсыну, зиянды бағдарламалық жасақтамадан «қорғау» үшін ыңғайлы «мүмкіндіктер» ретінде өтіп кетеді немесе егер сіз құрылғыңызды жоғалтсаңыз. Деректерді қорғаудың ең сенімді әдістерінің бірі Мүмкін емес миссия мақаласында сипатталған: Android-ті қауіпсіздік пен құпиялылық үшін қатайту, бірақ бұл телефон туралы емес, планшет туралы және тек WiFi қолдауымен (менің ойымша, бұл жерде блобсыз мобильді чиптер, мобильді Интернет үшін осы планшетпен бірге бөлек 3G-модемді пайдалану ұсынылады, ол блоктарға ешкім зиян келтірмейді, өйткені бұл модемде жеке деректер жоқ), және дәл корпус, физикалық түрде ажыратылған микрофон. Телефондағы жеке деректерді толықтай қорғаудың мүмкін еместігіне қарамастан, мен мүмкіндігінше максималды жұмыс жасау керек деп санаймын: мүмкіндігінше ағып жатқан арналарды жабыңыз - өйткені аз адамдар ұялы телефонды пайдаланбауға немесе жеке деректерін сақтауға мүмкіндігі жоқ. онда (ең болмағанда байланыс және қоңырау тарихы). Анонимдік туралы әңгіме мүлдем болмайтынын бірден түсіндіремін. Бұл жеке үлкен және күрделі тақырып, ол Tor-ды қолдануды, GSM-ден толық бас тартуды және барлық телефонияны шифрланған VoIP-ке ауыстыруды және т.б. қажет етеді. Бұл тақырып бойынша сіз алдыңғы сілтемені оқып, The Guardian Project қосымшаларын пайдалануыңыз керек. Бірақ мұның бәрін жасау мағынасы болуы мүмкін, егер сіздің деректеріңіз телефоннан тікелей ағып кетпесе, яғни. осы мақалада сипатталған мәселелерді шешкеннен кейін. Төменде сипатталған сәйкестендіруді / қадағалауды қорғау әдістері жасырындықты қамтамасыз етпейді, олар жай ғана жеке деректердің ағып кетуінің кейбір қосымша арналарын жасырады (ол сіз қай жерде және қашан болғаныңызды қамтиды). Тағы бір проблема - бұл қарапайым және қарапайым пайдаланушы үшін қол жетімді емес сипатталған шешімдердің ыңғайлылығы емес, күрделілігі. Оқырман телефонның микробағдарламасын қалай өзгерту керектігін, adb қолданбасын біледі және Linux командалық жолымен аз да болса таныс деп болжанады. Негізінде сипатталғандардың көпшілігі қарапайым пайдаланушыға бірнеше батырманы басу арқылы автоматтандырылып, қол жетімді бола алады, бірақ әзірге ешкім мұны істеген жоқ.
* 

Құрамы Қауіпсіздік әртүрлі элементтерден қалыптасады және олардың кез-келгеніне немқұрайлы қарау барлық күш-жігерді жоққа шығаруы мүмкін: • ОЖ және негізгі қосымшалар (сіздің жеке деректеріңізбен жұмыс) ашық қайнар көзден тұруы керек, әйтпесе оларға негізінен ешқандай сенім туралы мәселе туындауы мүмкін емес. • Сізде root-қатынас болуы керек (олар айтқандай, егер сіз компьютерде root болмасаңыз, онда басқа біреу root болып табылады ... және төменде сипатталған кейбір қосымшалар root-қатынасты қажет етеді). • ОЖ-ны және қосымшаларды бұзу мүмкіндігін азайту үшін үнемі жаңартып отыру қажет. • Жеке деректерді «синхрондаудың» орнына жүйелік сақтық көшірмелерді қолдану керек және сенімді түрде шифрланған. • Барлық қосымшалардың жеке деректерге қол жетімділігі шынымен қажетті минимуммен шектелуі керек, камераға / микрофонға қол жетімділікті бақылау керек. • Интернетке барлық қосымшалардың қол жетімділігі ең қажетті минимуммен шектелуі керек. • «әуе арқылы» деректерді беру қауіпсіз түрде жүзеге асырылуы керек: • «ауамен» берілетін барлық нәрселер шифрланған болуы керек (VPN-ге кіру керек); • Wi-Fi-ға қосылу дұрыс кіру нүктесіне қосылуымыз үшін қосымша сақтық шараларын қажет етеді; • Wi-Fi-мен жұмыс істеу бақылауға мүмкіндік беретін мәліметтердің ағып кетуінен қосымша қорғауды қажет етеді. • Жоғалған / ұрланған жағдайда телефондағы деректерді қорғау. OS ашық көзіне қойылатын талап iOS пен Windows Phone-ды дереу жоққа шығарады, және Android-ге негізделген опциялардың барлығы бірдей қолайлы бола бермейді. Мен CyanogenMod қолданамын, бірақ бұл жалғыз нұсқа емес (егер сіздің телефоныңызға репликант қолдау көрсететін болса, ол жақсырақ болуы мүмкін, сонымен қатар Firefox OS, Ubuntu Touch, Tizen бар). ОЖ-ның ең соңғы нұсқаларын қолдануға келетін болсақ, өкінішке орай, мен CyanogenMod 11-ді Android 4.4.4 (KitKat) негізінде орнатуға тура келді. Екі себеп бар: біріншіден, менің телефонымда Android 5.x жүйесінде CyanogenMod жоқ, екіншіден, Android 5.x жүйесіне арналған Xposed фреймворкінің әлі күнге дейін тұрақты нұсқасы жоқ. Сақтық көшірмелерді сенімді шифрлау үшін сізге Titanium Backup ақылы нұсқасы қажет болады. Қолданбалардың жеке деректерге қол жетімділігін толығымен бақылау үшін сізге XPrivacy ақылы нұсқасы қажет. Негізінде, сіз ақысызға қол жеткізе аласыз, бірақ бұл әлдеқайда күрделі болады (функциялар параметрлері және ақ-қара тізімдер туралы ақпарат қол жетімді басқаруға мүмкіндік береді, ал пакеттік операциялар көп уақытты үнемдейді). Мен оны жеке тексерген жоқпын, бірақ «ақылы» нұсқаны ақысыз алуға болатын сияқты (ақылы нұсқа сайтындағы парақтың соңындағы форма). GApps GApps туралы айтатын болсақ. Ең дұрысы, оны мүлдем орнатпаған дұрыс болар еді - егер сізде F-Droid-тен қосымшалар жеткілікті болса. Сіз NOGAPPS a.k.a арқылы өтіп көруге болады. Projectg жобасы, бірақ іс жүзінде Google Play дүкенін толыққанды ауыстыру жоқ (және оған NOGAPPS арқылы кіру кез келген уақытта сатып алынған қосымшалардың тыйым салынуына және жоғалуына әкелуі мүмкін, себебі бұл Google ережелерін бұзады). Бұл жағдайда сіз GApps-тің минималистік нұсқасын, қажет болса, басқа GApps қосымшаларын Play Store арқылы орнатқаныңыз жөн (егер бұл жағдайда олар қосымша орын алады деп алаңдасаңыз, онда, ең алдымен, бұл бәрібір қалады олар бірінші рет жаңартылған кезде орын алады, екіншіден, бұл мәселені шеше отырып, қосымшаларды / жүйеге ауыстыра алатын утилиталар, соның ішінде Titanium Backup бар). Тұтастай алғанда, қысқартылған GApps ассемблерін құрған әзірлеушілер бұл жиындарды одан әрі қолдаудан бас тарта бастағанын атап өту керек, бәрінде кенеттен отбасылық мәселелер болды, және қандай да бір себептермен, қолдаудан бас тартқаннан кейін біраз уақыт өтті. , олар орналастырылған файлдарды осы жиналыстар талқыланған алдыңғы жиындар мен форум тізбектерінен тұратын файлдардан жойды.



Осыған қарамастан, бірнеше нұсқаны табуға болады: jajb-дан минималистік жинақ (мен одан GoogleContactsSyncAdapter.apk, GoogleBackupTransport.apk және GoogleFeedback.apk файлдарын өшірер едім, бірақ оларсыз ешнәрсе бұзылмайтынына сенімдімін) және өте икемді және теңшелетін, бірақ бұдан былай Т.Круззеден П.А.Гаппс қолдамайды. Одан басқа, қажет емес файлдардың тізімін анықтау үшін қазірдің өзінде орнатылған GApp қолданбасынан «қажетсіз» қосымшаларды алып тастауға болады, ең қарапайым тәсілі - жоғарыда аталған PA Gapps-тің минималды және максималды нұсқаларын салыстыру.

* Микробағдарлама мен есептік жазбаларды ауыстыру Егер сіз телефонды қолданудың басынан бастап барлық сақтық шараларын қолданбасаңыз, онда сіздің жеке деректеріңіз әлдеқашан «ағып» кеткен және көптеген бейтаныс адамдар үшін қол жетімді. Бұл жағдайда сізге сипатталған қосымшаларды жай ғана орнатып, олармен тәжірибе жасап, өзіңізге сенімді болған кезде телефоннан барлық деректерді (ішкі / сыртқы SD картасының мазмұнын қоса) өшіріп, орнатқаныңыз жөн болар еді. бәрі нөлден - бұл сіздің деректеріңізді қайтарып алмайды, бірақ, ең болмағанда, осы деректер мен телефон арасындағы байланысты үзеді. Есептік жазбаларға келетін болсақ, микробағдарламаны ауыстырғаннан кейін сізге телефон, Google, Facebook және т.б.-да бөлек есептік жазбалар жасау қажет. Бұл әдеттегі тіркелгілерді қажетті қосымшаларда пайдалануға мүмкіндік бермейді, бірақ басқалар үшін бұл оларға қол жетімді деректер көлемін едәуір шектейді (мысалы, тек бірнеше ойындарда мен кіруге мүмкіндік берген «менің» Facebook) кейбір бонустар үшін).
* НАЗАР АУДАРЫҢЫЗ: егер сіз Play Store дүкенінен қосымшалар сатып алған болсаңыз, онда микробағдарламаны ауыстырғаннан кейін сол Google есептік жазбасын қолдансаңыз, қазірдің өзінде ағып кеткен деректер мен сіздің телефоныңыздың арасындағы байланыс қалады (кем дегенде Google үшін), ал егер есептік жазба жаңа болса, сіз бұрын сатып алынған қолданбаларды жоғалтасыз. Егер сізде микробағдарламаны ауыстыру және / немесе телефонға бөлек есептік жазбалар жасау тым көп болса, онда бұл дұрыс емес - мен басында жазғанымдай, телефондағы жеке деректерді толық және сенімді қорғаудың мүмкіндігі жоқ, тек қана қамту туралы деректердің мүмкіндігінше көп арналар ағып жатыр. Сіздің жағдайда қазіргі уақытта мүмкін болатыннан гөрі аз ғана арналар қамтылады. Бұдан әрі сіз қазіргі микробағдарламаны ауыстыруға шешім қабылдадыңыз деп ойлаймын - егер бұлай болмаса, сипатталған әрекеттерді өткізіп жіберіңіз. Бөлімдер Төменде сипатталған әрекеттерді түсіну үшін сізге Android-тің негізгі бөлімдері туралы минималды түсінік қажет. Қысқаша айтқанда, негізгі бөлімдер:

Жоғалған / ұрланған жағдайда телефондағы деректерді қорғау Телефонға физикалық қол жеткізген бөтен адамның сіздің жеке деректеріңізге кіруіне жол бермеу үшін сізге: • деректерді шифрлауды қосу • бұл үшін күрделі құпия сөзді қолданған жөн (әдепкі бойынша, дәл сол пароль құлыптау экранында қолданылады, бұл әдетте өте ыңғайсыз, бірақ оны шешу оңай және құлыптау экраны үшін басқа құпия сөзді / түйреуішті қолданады) • құлыптау экранында парольді немесе күрделі PIN кодты қолданыңыз • оны үнемі үйге кіргізбеу үшін Tasker көмегімен оны үйде болғанда автоматты түрде өшіріп, үйден шыққан кезде қосуға болады. • пайдаланылмаған кезде АДБ-ны (және АДБ үшін түбірлік рұқсаттарды) өшіріңіз • бұл Android 4.3-тен онша маңызды емес Өкінішке орай, ClockworkMod де, TWRP де құпия сөзбен қорғауды қолдамайды. Мұнсыз сіздің телефоныңызға уақытша қол жеткізген адам қалпына келтіру үшін қайта қосылып, троянмен / бумада қосымша пакет орнатып, содан кейін телефонды сізге қайтара алады. ОЖ жүктеліп, / деректерге арналған шифрлау паролін енгізген бойда, бұл троян root ретінде жұмыс істей алады және сіздің барлық жеке мәліметтеріңізге толық қол жеткізе алады. Егер қалпына келтіру құпия сөзбен қорғауды қолдаса, мұны істеу үшін сіз қалпына келтіруді қайтадан жыпылықтауы керек еді, бұл парольді қалпына келтіреді және телефон сізге қайтарылғаннан кейін араласу фактісін бақылауға мүмкіндік береді. Ұрыға қарсы «Ұрлыққа қарсы» және телефонды қашықтан басқару сияқты қосымшаларға қатысты. Бұл қосымшалар қарапайым, қорғалмаған телефонда әлі де мағынасы бар болуы мүмкін - егер ұры ақымақ болып ұсталса және SIM картасын лақтырып тастап, барлық бөлімдерін қайта пішімдеудің орнына, ол осы телефоннан Интернетте отырса және басқа адамдардың фотосуреттерін зерттесе .. Иә, бұл қосымшалардың артықшылықтары мүмкін. Бірақ біздің жағдайда ол деректерге қол жеткізе алмайды, демек, оларды қашықтықтан өшірудің қажеті жоқ (әсіресе қашықтан басқаруға арналған кез-келген қосымша шын мәнінде оның жеке деректерін дамыған компаниямен біріктірудің тағы бір әдісі болып саналады) қосымшасы). Телефонның орналасқан жерін анықтау мүмкіндігіне келетін болсақ - ол үшін Интернет болуы керек, содан бері ұры телефонның ОЖ-не қол жеткізе алмайды, содан кейін ол өзінің үйінде Wi-Fi байланысын орната алмайды және оның SIM картасын «пайдасыз телефонға» салуы екіталай. Оның сіздің SIM картаңызды лақтырып тастамауы немесе телефонға қосылған Wi-Fi ыстық нүктесінің жанында телефонды алып жүрмеу ықтималдығы ... менің ойымша, мұны күткендей емес, ол осы қолданбаны жасаған компанияның орналасқан жері туралы деректерді үнемі біріктіреді ... Егер телефон жай жоғалып кеткен болса, оны біреу тауып алып, оны иесіне қайтарғысы келсе, сіз байланыс мәліметтерін (мысалы, электрондық пошта) құлыптау экранында көрсетуіңіз керек немесе жай ғана қоңырау шалыңыз. Бірақ телефонды ұрлап алғаны белгілі болғаннан кейін бірден не істеу керек - SIM картаны бұғаттаңыз (ол 2 факторлы авторизацияны айналып өтуге немесе банктік төлемдерді SMS арқылы растауға пайдаланылмауы үшін) және, мүмкін, телефонды Google есептік жазбасынан ажыратыңыз. XPrivacy-ді теңшеу Жалпы алғанда, бұл осы мақалада сипатталғандардың бәрінен қиын. XPrivacy сізге көптеген операциялар мен деректерді басқаруға мүмкіндік береді, ал барлық қосымшалардың қажеттіліктері әртүрлі, ал көптеген қосымшалар үшін шектерді жеке-жеке өзгертуге тура келеді. Сонымен бірге, Android жасаушысы болып табылмайтын пайдаланушы үшін бұл операциялардың көпшілігі түсініксіз: олар қаншалықты маңызды, қандай деректерге қол жеткізуге мүмкіндік береді, осы операциялар осы қосымшаның жұмысы үшін шынымен қажет пе. Мен тек жалпы ұсыныстар бере аламын: • Менің тәжірибеме сүйенсек, қосымшалар үшін XPrivacy параметрлерін автоматты түрде шығарып алу үшін краудсорсинг қызметін қолдану жақсы идея емес. XPrivacy-ді конфигурациялау өте күрделі, сондықтан көптеген пайдаланушылар мұны өте жақсы жасамайды, бірақ өз параметрлерін осы қызметке жіберуге қуанышты. Басқалардың орташаланған параметрлерін сорып алу арқылы сіз бұғатталатын (және болуға тиіс) заттардың шамамен 10-20% -ын жауып тастайсыз. • XPrivacy-ді блоктау / қолдан жасауды білетін барлық нәрсе сіздің жеке деректеріңізге тікелей байланысты. Сондықтан мүмкіндігінше бәрін бұғаттауға тұрарлық. • «сарапшы» режимін бірден қосып, жүйелік қосымшаларды бұғаттауға мүмкіндік беру керек. • Ең шектеулі әдепкі шаблонды дайындаңыз - барлық санаттар мен операциялар үшін шектеулерді бұғаттауға және сұрауға мүмкіндік беріңіз (оның ішінде қауіпті): • Датчиктер - қауіпті операцияларға рұқсат етілуі мүмкін (барлық қолданбаларға қажет). • Құрылғыны идентификациялау - бәрін блоктаңыз, бірақ сіз бұған рұқсат етілмейтін заттар үшін шектеулер туралы сұранысты өшіру керек. • Интернет - inet\_ \* қоспағанда, барлық қауіпті операцияларға рұқсат берген жөн (барлық қолданбаларға қажет, сонымен қатар Интернетке кіру брандмауэрмен басқарылатын болады). • Жүйе (мұрт) интернет.


* проверьте, и при необходимости повторно отключите Wi-Fi, мобильный  интернет и определение местоположения
* активируйте ADB:
	+ Настройки → О телефоне → 7 тапов по Номер сборки
	+ Настройки → Для разработчиков → [✓] Отладка по сети & USB
	+ Настройки → Для разработчиков → Режим суперпользователя → Для  приложений и ADB
* если у вас раздел /data не был зашифрован или вы его переформатировали  в процессе прошивки CyanogenMod — зашифруйте его (если это делать так, а  не через интерфейс, то можно задать пароль шифрования отличающийся от  пароля/пин-кода экрана блокировки):
	+ adb root
	+ adb shell vdc cryptfs enablecrypto inplace <пароль>
	+ подождите пока система зашифрует /data и снова загрузится
* Настройки → Безопасность → [✓] Неизвестные источники
* Скачайте на компьютер и установите через adb install (чтобы пока не  установлены XPrivacy и AFWall+ не включать на телефоне интернет)  [Xposed  framework](http://repo.xposed.info/module/de.robv.android.xposed.installer).
	+ Фреймворк → Установить/Обновить
	+ перезагрузите телефон
	+ скачайте скрипт  [90-xposed.sh](http://forum.xda-developers.com/showpost.php?p=43473060),  который будет сохранять Xposed framework при OTA-обновлениях  CyanogenMod, и установите его:
		1. adb root
		2. adb shell mount -o remount,rw /system
		3. adb push 90-xposed.sh /system/addon.d/
		4. adb shell chmod 0755 /system/addon.d/90-xposed.sh
		5. adb shell mount -o remount,ro /system
* Скачайте на компьютер и установите через adb install  [XPrivacy](http://repo.xposed.info/module/biz.bokhorst.xprivacy).
	+ установите его лицензию залив /sdcard/XPrivacy\_license.txt
		1. если это делается при активном XPrivacy — перезагрузите телефон
	+ активируйте модуль XPrivacy в Xposed framework
	+ запустите один раз XPrivacy
	+ перезагрузите телефон
	+ Меню → Параметры → [✓] Режим эксперта
	+ Меню → Параметры → Режим эксперта → [✓] Запрет системных компонентов
	+ Меню → Параметры → Режим эксперта → [✓] Режим AOSP
	+ перезагрузите телефон
	+ настройте XPrivacy максимально ограничив доступ всем приложениям  включая системные (рекомендации по настройке описаны выше)
* В зависимости от используемой вами прошивки может потребоваться  установить [BusyBox](https://f-droid.org/wiki/page/stericson.busybox) (в  CyanogenMod 11 он уже есть).
* Скачайте на компьютер и установите через adb install  [AFWall+](https://f-droid.org/repository/browse/?fdid=dev.ukanth.ufirewall).
	+ Меню → Настройки → [✓] Активные правила
	+ Меню → Настройки → [✓] Управление VPN
	+ Меню → Настройки → [✓] Поддержка IPv6 (пользоваться им не  обязательно, но файрволить нужно, иначе приложения которым закрыт  доступ файрволом через IPv4 без проблем выйдут в интернет через IPv6)
	+ Меню → Настройки → [✓] Администратор устройства
	+ Меню → Настройки → Экспериментальные: [✓] Исправить утечку данных  при запуске. Это установит скрипт /system/etc/init.d/afwallstart  блокирующий доступ в интернет пока OS загружается и AFWall+ ещё не  запустился.
	+ Меню → Включить брандмауэр
		1. режим Белый список (разрешить выбранные), а поскольку выбранных пока  нет — всем приложениями доступ пока что закрыт
* Нам нужно позаботится, чтобы /system/etc/init.d/afwallstart не был  удалён при OTA-обновлении OS. Для этого создадим свой скрипт  /system/addon.d/99-local.sh, в который будем добавлять имена файлов на  разделе /system, которые нужно сохранить при OTA-обновлении:
	+ adb root
	+ adb shell mount -o remount,rw /system
	+ adb shell cp /system/addon.d/50-cm.sh /system/addon.d/99-local.sh
	+ отредактируйте /system/addon.d/99-local.sh, заменив в функции  list\_files() файл etc/hosts на etc/init.d/afwallstart
	+ adb shell mount -o remount,ro /system

Если вы ещё не прошили GApps — сделайте это сейчас. После загрузки настройте ограничения XPrivacy для приложений GApps.

Настраиваем систему:

* Настройки Google → Безопасность → [ ] Удалённая блокировка и сброс
* Настройки Google → Безопасность → [ ] Борьба с вредоносными  приложениями
* Настройки → Беспроводные сети: Передача данных → Меню → [ ]  Автосинхронизация данных
* Настройки → Беспроводные сети: Ещё… → [ ] Режим полёта
	+ отключаем временно, только для того чтобы переключить следующий пункт
* Настройки → Беспроводные сети: Ещё… → [ ] NFC
* Настройки → Беспроводные сети: Ещё… → [✓] Режим полёта
* Настройки → Экран блокировки → Безопасность экрана → Блокировка экрана
	+ установить надёжный пароль или пин-код
* Настройки → Местоположение (выкл.)
* Настройки → Безопасность → Администраторы устройства → [ ] Удалённое  управление Android
* Настройки → Безопасность → Администраторы устройства → [✓] XPrivacy
* Настройки → Безопасность → Администраторы устройства → [✓] AFWall+
* Настройки → Конфиденциальность → Отправка статистики → [ ] Включить  отправку отчётов
* Настройки → Язык и ввод → Проверка правописания (настройки) → Проверка  правописания Android (настройки) → [ ] Поиск контактов
* Настройки → Язык и ввод → Клавиатура Android (настройки) → Расширенные  настройки → [ ] Подсказывать имена
* Если вы ставили не минимальный вариант GApps, то где-то рядом должна  быть аналогичная настройка для Google Voice — её тоже выключить.
* Настройки → Восстановление и сброс → [✓] Резервирование данных
	+ включаем временно, только для того чтобы переключить следующий пункт
* Настройки → Восстановление и сброс → [ ] Автовосстановление
* Настройки → Восстановление и сброс → [ ] Резервирование данных
* Настройки → Для разработчиков → Сетевое имя устройства → localhost
* Телефон → Меню → Настройки → [ ] Прямой поиск
* Телефон → Меню → Настройки → [ ] Поиск контактов
* Телефон → Меню → Настройки → [ ] Обратный поиск

Подключаем интернет:

* Перед открытием доступа к интернет стоит заблокировать некоторые  приложения, в частности:
	+ Настройки → Приложения → Все → Синхронизация Контактов Google →  Отключить
	+ Настройки → Приложения → Все → Google Резервное копирование →  Отключить
* Скачайте на компьютер и установите через adb install:
	+ [Wi-Fi  Privacy Police](https://f-droid.org/repository/browse/?fdid=be.uhasselt.privacypolice)
	+ [Pry-Fi](https://play.google.com/store/apps/details?id=eu.chainfire.pryfi)
	+ [AdAway](https://f-droid.org/repository/browse/?fdid=org.adaway)
	+ [F-Droid](http://f-droid.org/)
	+ [OpenVPN  for Android](https://f-droid.org/repository/browse/?fdid=de.blinkt.openvpn) или любой другой VPN и настройте его
* Разрешите в AFWall+ доступ к Wi-Fi только для одного приложения:
	+ OpenVPN for Android
* Разрешите в AFWall+ доступ к VPN для:
	+ (NTP) — опционально
	+ AdAway
	+ F-Droid
	+ Google Play Маркет
	+ Xposed Installer
	+ Загрузки, Хранилище мультимедиа, Диспетчер загрузки
	+ Обновление CyanogenMod
* Для первой активации аккаунта Google нужно дать доступ к VPN для:
	+ Аккаунты Google, Сервисы Google Play, Google Резервное копирование,  Google Services Framework, Синхронизация Контактов Google
* Включите Wi-Fi или мобильный интернет.
* Активируйте VPN.
* Создайте или подключите существующий аккаунт Google (чтобы инициировать  добавление аккаунта можно например запустить Play Маркет).
* Настройки → Аккаунты → Google → ваш аккаунт → выключить всю  синхронизацию
* Настройки Google: отключить всё, кроме:
	+ Подключенные приложения
	+ Play Игры

Теперь можно отключить доступ к VPN для «Аккаунты Google, Сервисы Google Play, Google Резервное копирование, Google Services Framework, Синхронизация Контактов Google». Этот набор приложений — один из основных каналов утечки личных данных. Доступ в интернет ему нужен для:

* обновления просроченного токена доступа к гугл-аккаунту
* поддержки GCM (Google Cloud Messaging — пуш-уведомлений Android)
* активного сливания всех ваших личных данных, до которых он дотянется

Для обновление токена нужно открывать ему доступ крайне редко и ненадолго. Что касается GCM, то, с одной стороны, пуш-уведомления нужны для работы многих приложений, так что вы можете захотеть оставить ему доступ к VPN. С другой стороны, если вы дадите какому-то приложению хоть раз ненадолго доступ в интернет, то оно может зарегистрироваться в GCM и после этого будет получать пуш-уведомления (через этот набор приложений гугла) даже если вы ему доступ в интернет заблокируете. Хорошо это или плохо — решайте сами. Лично мне не нравится идея, что отключенное от интернета приложение продолжает получать из интернета данные, но хотя бы оно не сможет ничего отправлять.

Для защиты от [фоновой установки](https://nakedsecurity.sophos.com/2011/02/04/android-market-web-store-backdoor-phone-hackers/) программ на ваш телефон по желанию гугла, доступ в интернет для «Google Play Маркет» нужно разрешать только непосредственно тогда, когда вы им пользуетесь.

Для того, чтобы видеть полную информацию по запрашиваемым правам доступа для устанавливаемых из Play Маркет приложений нужно установить модуль для Xposed framework [PlayPermissionsExposed](http://forum.xda-developers.com/xposed/modules/playpermissionsexposed-fix-play-store-t2783076) и перезагрузить телефон.

Установить из Play Маркет:

* [SRT  AppScanner](https://play.google.com/store/apps/details?id=de.backessrt.appintegrity)
	+ запустить его, если он найдёт уязвимость — установить модуль Xposed  [Master  Key multi-fix](http://repo.xposed.info/module/tungstwenty.xposed.masterkeydualfix)
* [Secure  Update Scanner](https://play.google.com/store/apps/details?id=com.iu.seccheck)
* [Titanium  Backup ★ root](https://play.google.com/store/apps/details?id=com.keramidas.TitaniumBackup)
* [Titanium  Backup PRO Key ★ root](https://play.google.com/store/apps/details?id=com.keramidas.TitaniumBackupPro)

Сейчас самое время перегрузиться в recovery и сделать полный бэкап новой системы!

Восстановить из бэкапов Titanium Backup все нужные приложения. Запустить из меню Titanium Backup «Маркет доктор» для восстановления связей этих приложений с Play Маркет.

Теперь можно отключить ADB и запретить для него права root.

Поздравляю! У вас в руках Android-телефон, защищённый от утечек личных данных настолько, насколько это вообще возможно без отказа от доступа к Play Маркет и GSM-связи.