

НАКАЗ

ГОЛОВНОКОМАНДУВАЧА ЗБРОЙНИХ СИЛ УКРАЇНИ

29.04.2024

м. Київ

№ 165

Про затвердження Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами

Відповідно до Указу Президента України “Питання Головнокомандувача Збройних Сил України” від 27 березня 2020 року № 123/2020, з метою визначення порядку зберігання і користування мобільними комунікаційними пристроями та іншими електронними засобами, вжиття заходів із захисту інформації особовим складом Збройних Сил України,

НАКАЗУЮ:

1. Затвердити Інструкцію зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами, що додається.

2. Визнати таким, що втратив чинність наказ Головнокомандувача Збройних Сил України від 01 квітня 2020 року № 74 “Про затвердження Інструкції зі зберігання і користування особовим складом Збройних Сил України засобами стільникового зв'язку та іншими електронними засобами”.

3. Наказ розіслати згідно з розрахунком розсилки.

Головнокомандувач Збройних Сил України
генерал-полковник



Олександр СИРСЬКИЙ

ЗАТВЕРДЖЕНО

Наказ Головнокомандувача
Збройних Сил України29 квітня 2024 року № 165

ІНСТРУКЦІЯ

зі зберігання і користування особовим складом Збройних Сил України
мобільними комунікаційними пристроями та іншими електронними засобами

1. Загальні положення

1.1. Ця Інструкція визначає порядок зберігання і користування мобільними комунікаційними пристроями та іншими електронними засобами військовослужбовцями та працівниками Збройних Сил України, які виконують обов'язки військової служби, державної служби (праці) у Збройних Силах України в пунктах постійної дислокації органів військового управління, військових частин та установ Збройних Сил України, під час навчального процесу, проведення занять, навчань, тренувань та інших заходів підготовки, у районах виконання бойових (спеціальних) завдань та у районах відновлення боєздатності.

1.2. У цій Інструкції нижченаведені терміни вживаються в такому значенні:
особовий склад Збройних Сил України – військовослужбовці та працівники Збройних Сил України;

інформація з обмеженим доступом – інформація, що становить передбачену законом таємницю, службова інформація, конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”;

месенджери – програмне забезпечення (мобільний додаток) для обміну повідомленнями, яке дозволяє відправляти текстові повідомлення, зображення, відео, аудіофайли, а також робити голосові та відеодзвінки через мережу Інтернет. Вони можуть включати такі функції, як обмін файлами, геолокація, веб-конференції та місця для зберігання даних;

мобільні комунікаційні пристрої (далі – МКП) – радіоприймальні та радіопередавальні пристрої, що приймають (передають) інформацію та дані по безпроводових каналах зв'язку стандартів GSM, UMTS, WCDMA, LTE, CDMA та інших стандартів загального користування (засоби стільникового зв'язку, планшети, портативні персональні комп'ютери тощо);

інші електронні засоби (далі – ІЕЗ) – пристрої, крім МКП, які мають будь-яку з функцій: запису фото-, відео- та аудіоінформації, обробки та зберігання інформації у цифровому вигляді, визначення геолокації, обміну інформацією по безпроводових та проводових (оптоволоконних) каналах зв'язку (трекери, смарт-годинники тощо);

спеціально налаштовані мобільні комунікаційні пристрої та інші електронні засоби (далі – СН МКП та ІЕЗ) – налаштовані згідно з рекомендаціями з налаштування особистих мобільних комунікаційних пристроїв (додаток 1), радіоприймальні та радіопередавальні пристрої, що приймають (передають) інформацію та дані по безпроводових каналах зв'язку стандартів GSM, UMTS, WCDMA, LTE, CDMA та інших стандартів загального користування, що використовуються виключно в службових цілях, номер телефону якого не прив'язаний до фінансових установ. На спеціально налаштовані МКП та ІЕЗ заборонено встановлювати додатки соціальних мереж (TikTok, Instagram, Facebook тощо) та будь-які месенджери, окрім Signal, WhatsApp та Threema;

кібербезпека Збройних Сил України – захищеність життєво важливих інтересів військовослужбовців та працівників військових організаційних структур Збройних Сил України під час виконання бойових та спеціальних завдань, заходів повсякденної діяльності з використанням кіберпростору, за якої забезпечується стале надання інформаційних та комунікаційних сервісів та своєчасне виявлення, запобігання та нейтралізація реальних і потенційних кіберзагроз безпеці операцій та повсякденній діяльності військ (сил) Збройних Сил України.

1.3. Вимоги цієї Інструкції є обов'язковими для виконання особовим складом Збройних Сил України, який перебуває на території органів військового управління, з'єднань, військових частин, військових навчальних закладів, установ та організацій Збройних Сил України, а також на пунктах управління угруповань військ (сил), військових частин та в районах виконання бойових (спеціальних) завдань.

Всі військовослужбовці зобов'язані враховувати ризики, на які вони наражають себе, родину, колег або операцію, коли публікують інформацію в інтернеті або передають її у месенджерах, у повідомленнях електронною поштою тощо. Інформація та/або зображення можуть окремо або спільно з іншою інформацією давати уявлення про поточні операції, обладнання, можливості, тактику та наміри Збройних Сил України.

1.4. Перебування особового складу Збройних Сил України та інших осіб на/в об'єктах інформаційної діяльності з МКП та ІЕЗ, що не входять до складу цього об'єкту інформаційної діяльності, – заборонено.

1.5. Об'єкти інформаційної діяльності позначаються відповідними попереджувальними знаками із написом (додаток 4). Попереджувальні знаки

розміщуються в місцях входу у зазначені об'єкти.

1.6. Передача інформації з обмеженим доступом під час ведення переговорів з використанням МКП та ІЕЗ, не обладнаних сертифікованими в Україні засобами криптографічного захисту інформації, а також в умовах, коли конфіденційність переговорів не забезпечується, забороняється.

1.7 Заборонено здійснювати підключення особистих та СН МКП та ІЕЗ до електронних комунікаційних, інформаційних, інформаційно-комунікаційних, автоматизованих систем та систем спеціального зв'язку Збройних Сил України, за винятком мереж, призначених для надання доступу користувачам до мережі інтернет та налаштованих відповідно до вимог Порядку організації кіберзахисту інформаційно-комунікаційних систем пунктів управління органів військового управління Збройних Сил України.

1.8. За порушення вимог Інструкції військовослужбовці та працівники Збройних Сил України несуть персональну відповідальність.

У разі невиконання або неналежного виконання вимог Інструкції командиром (начальником) може бути призначено службове розслідування (перевірка), за результатами якого командиром (начальником) приймається рішення про притягнення винних посадових осіб до відповідальності.

Якщо за результатами проведення службового розслідування (перевірки) встановлено факти витоку або передумови до витоку інформації з обмеженим доступом, командири (начальники) можуть ініціювати клопотання перед Службою безпеки України про скасування допуску до державної таємниці таким посадовим особам, разом із письмовим повідомленням із зазначенням причин і підстав для такого скасування.

1.9. Організація та забезпечення виконання вимог Інструкції покладається на керівників (командирів, начальників) військових організаційних структур або на визначеного ним заступника та на служби захисту інформації в автоматизованих системах. На пунктах управління – на керівників пунктів управління та їх структурних підрозділів.

1.10. Контроль за виконанням вимог цієї Інструкції покладається: підпорядкованим особовим складом – на їх безпосередніх керівників (командирів, начальників);

оперативним складом пунктів управління – на керівників структурних підрозділів (оперативних груп) пунктів управління;

учасниками нарад, конференцій, занять та інших заходів – на керівників зазначених заходів;

особами на об'єктах інформаційної діяльності – на посадових (службових) осіб, відповідальних за зазначені об'єкти.

1.11. Контроль за правильністю налаштування МКП та ІЕЗ військовослужбовців та проведення періодичних перевірок дотримання вимог цієї Інструкції та рекомендацій у сфері кіберзахисту (додаток 1) покладається на служби захисту інформації в автоматизованих системах. До таких перевірок можуть залучатись представники підрозділів охорони державної таємниці, представники підрозділів кібербезпеки та інші підрозділи за рішенням відповідних командирів (начальників).

1.12. Особовий склад Збройних Сил України та особовий склад інших складових Сил оборони, що перебувають в оперативному підпорядкуванні в військових організаційних структурах Збройних Сил України повинні надавати СН МКП та ІЕЗ зазначеним службовим особам на їх вимогу для перевірки відповідних налаштувань.

2. Користування МКП та ІЕЗ у пунктах постійної дислокації

2.1. Дозволяється користуватися СН МКП та ІЕЗ у визначених керівником органу військового управління, командиром (начальником) військової частини (установи) місцях, також дозволяється користуватися МКП та ІЕЗ з функціями криптографічного захисту інформації, що допущенні до експлуатації та мають сертифікат відповідності, порядок користування яких визначається окремими інструкціями.

2.2. Порядок зберігання і користування особистими МКП та ІЕЗ для підпорядкованих військовослужбовців та працівників Збройних Сил України чи інших осіб, що перебувають на території органів військового управління, військових частин (установ) та навчальних закладів, встановлюється керівником органу військового управління, командиром (начальником) військової частини (установи), керівниками навчальних закладів шляхом видання відповідного наказу, який доводиться до всього особового складу органу військового управління (військової частини, установи) під особистий підпис.

2.3 На території органів військового управління, військових частин (установ), навчальних закладів особисті МКП та необліковані ІЕЗ, які мають функції запису фото-, відео- та аудіофіксації, визначення геолокації та функції підключення до мережі інтернет, здаються на тимчасове зберігання у вимкненому стані.

2.4. Тимчасове зберігання особистих МКП та ІЕЗ в органах військового управління організовується та здійснюється у спеціально обладнаних для цього місцях, оснащених шафами з окремими чарунками для МКП та ІЕЗ постійного особового складу органів військового управління та відвідувачів. Чарунки мають замикатися. Для МКП та ІЕЗ відвідувачів у місцях зберігання передбачається необхідна кількість чарунок, позначених написом «Відвідувач».

Місця для тимчасового зберігання МКП та ІЕЗ визначаються керівниками структурних підрозділів органів військового управління та за необхідності обладнуються системами відеоспостереження з виведенням на монітори чергових органів військового управління (структурних підрозділів органів військового управління) або іншими системами охорони.

Під час проведення нарад, конференцій та інших короткострокових заходів у визначених приміщеннях дозволяється організовувати тимчасове зберігання МКП у ящиках, розділених на чарунки, розташованих біля входу в зазначене приміщення, з видачею відвідувачу жетона-замінника із зазначеним на ньому номером чарунки.

2.5. Порядок тимчасового зберігання МКП та ІЕЗ у військових навчальних закладах, військових частинах (установах), а також в органах військового управління щодо забезпечення шафами з окремими чарунками для МКП та ІЕЗ визначається керівниками органів військового управління, військових навчальних закладів, командирами (начальниками) військових частин (установ). При цьому визначений порядок має унеможливлювати ведення несанкціонованого запису інформації у будь-якій формі, несанкціонованого доступу до об'єктів інформаційної діяльності та до глобальних мереж передачі даних, а також інших дій, що створюють передумови для витоку інформації з обмеженим доступом.

3. Користування МКП та ІЕЗ під час навчального процесу, проведення занять, навчань, тренувань та інших заходів підготовки (відновлення боєздатності)

3.1. Під час навчального процесу, проведення занять, навчань, тренувань та інших заходів підготовки користуватися особистими МКП та необлікованими, в тому числі особистими ІЕЗ, що мають функції запису фото-, відеофіксації та функції підключення до мережі інтернет, – забороняється.

3.2. Під час навчального процесу, проведення занять, навчань, тренувань та інших заходів підготовки дозволяється користуватися СН МКП у визначеному керівником занять порядку, також дозволяється користуватися МКП та ІЕЗ з функціями криптографічного захисту інформації що допущенні до експлуатації та мають сертифікат відповідності, порядок користування яких визначається окремими інструкціями.

3.3. Під час переміщення в район проведення занять, навчань, тренувань, інших заходів підготовки, які проводяться поза межами пунктів постійної дислокації, військовослужбовці повинні здати (у разі наявності) особисті МКП та ІЕЗ на тимчасове зберігання визначеній посадовій особі військової частини.

При цьому визначений керівником занять порядок має унеможливлювати ведення несанкціонованого запису інформації у будь-якій формі,

несанкціонованого доступу до об'єктів інформаційної діяльності та до глобальних мереж передачі даних, а також інших дій, що створюють передумови для витоку інформації з обмеженим доступом.

3.4. У районі проведення занять, навчань, тренувань, інших заходів підготовки, які проводяться поза межами пунктів постійної дислокації, заборонено використовувати стільникові мережі національних мобільних операторів зв'язку. Всі МКП та ІЕЗ мають підключатись до мережі Інтернет з дотриманням вимог Порядку використання локальних радіомереж в системі Міністерства оборони України та Порядку організації кіберзахисту інформаційно-комунікаційних систем пунктів управління органів військового управління Збройних Сил України.

4. Користування МКП та ІЕЗ на пунктах управління угруповань військ (сил)

4.1 На пунктах управління Генерального штабу Збройних Сил України, угруповань військ (сил) користування особистими МКП та ІЕЗ – заборонено.

4.2. Порядок зберігання і користування особистими МКП та ІЕЗ для підпорядкованих військовослужбовців та працівників Збройних Сил України чи інших осіб, що перебувають на території пунктів управління, визначається керівником пункту управління шляхом видання відповідного наказу (розпорядження), який доводиться до всього особового складу пункту під особистий підпис.

4.3 Дозволяється користуватися лише СН МКП та ІЕЗ у визначених керівником (командиром, начальником) пункту управління місцях, також дозволяється користуватися МКП та ІЕЗ з функціями криптографічного захисту інформації, що допущенні до експлуатації та мають сертифікат відповідності, порядок користування яких визначається окремими інструкціями. Під час користування зазначеними пристроями необхідно дотримуватись політик кібербезпеки.

4.4. У межах пункту управління заборонено використовувати стільникові мережі національних мобільних операторів зв'язку. Всі МКП та ІЕЗ мають підключатись до мережі Інтернет з дотриманням вимог Порядку використання локальних радіомереж в системі Міністерства оборони України та Порядку організації кіберзахисту інформаційно-комунікаційних систем пунктів управління органів військового управління Збройних Сил України.

4.5 Первинне конфігурування спеціально налаштованих МКП та ІЕЗ на пункті управління здійснюється представниками служб захисту інформації в автоматизованих системах органів військового управління (структурних

підрозділів органів військового управління). Інформаційно-телекомунікаційний вузол зв'язку пункту управління (далі – ІТВ ПУ) складає та веде перелік спеціально налаштованих МКП та ІЕЗ за формою, визначеною у додатку 5 під час підключення МКП та ІЕЗ до мереж ПУ. У разі потреби підрозділ ІТВ ПУ надає інформацію з цього переліку службі захисту інформації в автоматизованих системах ПУ та/або групі контролю за захистом інформації та кібербезпекою ПУ.

4.6 У разі використання месенджерів, дозволяється використовувати виключно Signal, WhatsApp та Threema, які спеціально налаштовані у відповідності до рекомендацій (додаток 1).

4.7 Під час користування спеціально налаштованими МКП заборонено зберігати відомості за якими можна ідентифікувати:

органи військового управління угруповань військ (сил) та військові частини (їх підрозділи), їх геопросторові дані, характер завдань та сили і засоби, що залучені до їх виконання;

осіб, місце проходження служби та характер завдань, що виконуються ними.

4.8 Зберігання особистих МКП та ІЕЗ на пунктах управління організовується та здійснюється у спеціально обладнаних для цього місцях, оснащених шафами з окремими чарунками для МКП та ІЕЗ оперативного складу пунктів управління. Чарунки мають замикатися, пристрої мають бути вимкнені.

Місця для зберігання МКП та ІЕЗ визначаються керівником пункту управління або керівниками структурних підрозділів (оперативних груп) пунктів управління.

4.9 Організація та забезпечення контролю за захистом інформації та кібербезпекою на пунктах управління покладається на службу захисту інформації в автоматизованих системах та/або на групу контролю за захистом інформації та кібербезпекою пункту управління, що створюється за рішенням керівника пункту управління.

4.10 Перевірки з дотримання вимог Інструкції проводяться з періодичністю, визначеною керівником пункту управління.

5. Користування МКП та ІЕЗ у районах ведення бойових дій

5.1 У районах ведення бойових дій користування особистими МКП та ІЕЗ, – заборонено.

5.2 Дозволяється користуватися лише СН МКП та ІЕЗ у порядку, визначеному керівником угруповання (командиром військової частини) шляхом видання відповідного наказу, який доводиться до всього підпорядкованого

особового складу. Також дозволяється користуватися МКП та ІЕЗ з функціями криптографічного захисту інформації, що допущенні до експлуатації та мають сертифікат відповідності, порядок користування яких визначається окремими інструкціями.

5.3 Під час користування спеціально налаштованими МКП заборонено зберігати відомості, за якими можна ідентифікувати:

органи військового управління угруповань військ (сил) та військові частини (їх підрозділи), їх геопросторові дані, характер завдань та сили і засоби, що залучені до їх виконання;

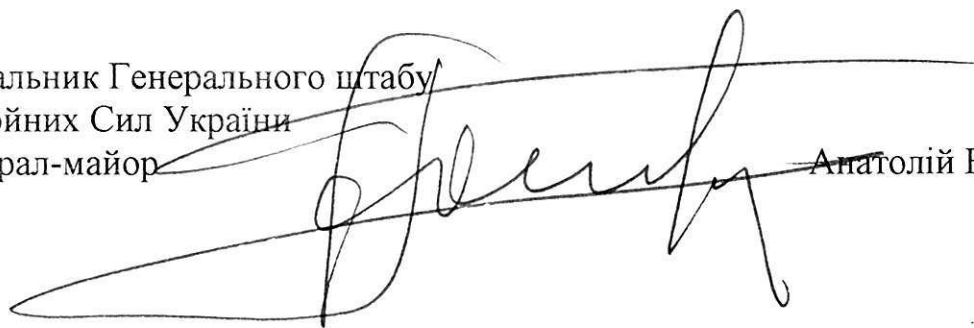
осіб, місце проходження служби та характер завдань, що ними виконується.

5.4 Зберігання особистих МКП та ІЕЗ у військових частинах (окремих підрозділах військових частин) організовується та здійснюється у спеціально обладнаних для цього місцях.

Місця для зберігання особистих МКП та ІЕЗ визначаються командирами військових частин або командирами окремих підрозділів військових частин.

6. Особливості використання МКП та ІЕЗ підрозділами сил спеціальних операцій, десантно-штурмових військ, морської піхоти, повітряних сил, підрозділів протиповітряної оборони, армійської авіації, ракетних військ і артилерії з урахуванням специфіки бойових (спеціальних) завдань (операцій) за необхідності можуть визначатися наказами відповідних командувачів, погоджених з Генеральним штабом Збройних Сил України.

Начальник Генерального штабу
Збройних Сил України
генерал-майор



Анатолій БАРГИЛЕВИЧ

Додаток 1

До Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами (пункти 1.2, 4.6)

РЕКОМЕНДАЦІЇ
щодо підвищення безпеки користування
мобільними комунікаційними пристроями
у Збройних Силах України

1. Загальні положення

Мобільні комунікаційні пристрої (далі – МКП), такі як стільникові телефони, планшети тощо, завжди мають притаманні їм вразливості, що пов'язані з особливостями технічної реалізації їх модулів, властивостей технологій передачі даних та недосконалостей програмного забезпечення. Відповідно, противник потенційно може використовувати такі вразливості для здійснення негативного кібервпливу на МКП.

Основними загрозами при користуванні МКП є:

отримання даних геолокації – як щодо безпосереднього місця знаходження МКП, так й відміток щодо місця та часу де й коли були зроблені фото- та відеоматеріали, які зберігаються на МКП;

перехоплення сесій та приховане підключення додаткових пристроїв у месенджерах на МКП, що може призвести до викриття конфіденційних даних, викрадення особистої інформації, а також можуть бути використані для шантажу або в інших злочинних цілях;

отримання противником віддаленого доступу до інформації, що зберігається у МКП (*списку контактів, журналів дзвінків (що дозволяє за частотою дзвінків визначити найближче коло спілкування); документів, фото- та відеоматеріалів, чатів та в месенджерах та СМС-листування, що зберігаються на МКП; збережених паролів до облікових записів тощо*), шляхом зламу МКП різними способами або зараження його шкідливими програмами через використання методів соціальної інженерії, розсилання фішингових листів, розміщення інфікованих додатків в App Store, Google Play, тощо;

отримання противником доступу до вищезгаданої інформації у разі фізичного захоплення МКП;

перехоплення дзвінків та листування як за допомогою провайдерів (операторів) електронних комунікаційних послуг, так й за допомогою спеціального програмного забезпечення та апаратури (*створення фейкових базових станцій стільникового зв'язку, фейкових точок доступу до безпроводних мереж, пристроїв Bluetooth, прихованим встановленням програм, що записують звук при розмові або роблять скріншоти при листуванні та потай пересилають їх на визначені інтернет-адреси, тощо*);

отримання доступу до камери та мікрофону смартфона та можливості, непомітно прослуховувати та бачити те, що відбувається навколо МКП (навіть коли МКП вимкнений);

використання рекламного ідентифікатора (*Advertising ID*), що дозволяє противнику стежити за активністю користувачів і створювати детальні профілі їхньої поведінки в інтернеті;

отримання доступу до керування МКП (*несанкціоноване вмикання та вимкнення МКП, стільникового зв'язку, Wi-Fi, Bluetooth, Airdrop, встановлення, запуск та видалення програм, зміна їх параметрів та параметрів МКП тощо*).

Дані рекомендації розроблені управлінням кібербезпеки Головного управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України з метою мінімізації вище перелічених загроз.

Важливо: деякі з наведених кроків налаштування МКП можуть мати інше найменування опцій залежно від виробника пристрою та версії операційної системи, але загалом принцип здійснення налаштування подібний.

При виникненні ускладнень у пошуку певних кроків налаштування пропонується користуватися функцією **Пошук налаштувань** (або **Пошук**) у програмі **Налаштування**. Пошук здійснюється по ключових словах, наприклад у віконці пошуку ввести "геолокація" і здійснити вибір серед запропонованих варіантів для подальших налаштувань.

2. Загальні рекомендації користувачу щодо безпечного використання та підвищення рівня безпеки користування МКП:

при виконанні завдань у недовіреному середовищі або у безпосередній близькості до противника не використовувати технологій біометричної автентифікації для розблокування МКП (розпізнавання обличчя – Face ID, відбиток пальця – Fingerprint ID) (існують ризики можливості розблокування пристрою без згоди користувача, наприклад уві сні, при втраті свідомості або загибелі), натомість використовувати графічний ключ, PIN-код або пароль;

не використовувати вживані МКП невідомих власників;

використовувати тільки МКП, які підтримуються виробниками та мають можливість отримувати оновлення безпеки для встановленої операційної системи;

регулярно оновлювати операційну систему МКП та встановлені програми, що дозволить усунути виявлені виробниками програмних продуктів вразливості;

не використовувати МКП, на яких здійснена "перепрошивка" операційної системи (*джейлбрейк для iPhone, надання прав суперкористувача Android (root)*);

використовувати зарядні пристрої тільки власні або довірених осіб;

запобігати доступу сторонніх осіб до МКП та не залишати його без нагляду;

перезавантажувати МКП не рідше одного разу на тиждень;

за відсутності потреби нагального використання МКП – вимикати його, якщо дозволяє конструкція МКП – також від'єднувати акумуляторну батарею;

якщо стільниковий зв'язок не потрібен, але є потреба у Wi-Fi-підключенні або Bluetooth – перевести МКП в режим польоту, після цього увімкнути необхідну функцію;

не підключати особисті МКП до службових (відомчих) засобів обробки інформації;

не підключати МКП до чужих комп'ютерів, не підключати до МКП чужих USB-пристроїв;

якщо відсутня необхідність користування камерами МКП – заклеїти їх непрозорим матеріалом;

не обговорювати важливі службові питання при наявності поблизу МКП; при неможливості – закривати мікрофон МКП щільним матеріалом або рукою;

не відповідати на дзвінки, повідомлення, електронні листи адресатів, що не входять до списку контактів;

не переходити за посиланнями, отриманими у повідомленнях (SMS, месенджерах), поштових повідомленнях, особливо від адресатів, що не входять до списку контактів;

не зберігати на МКП “чутливі” дані, неконтрольоване розповсюдження яких здатне нанести шкоду, особливо такі, що стосуються службової діяльності (*фото техніки та документів, характерних ознак місця перебування, персональні дані військовослужбовців, тощо*);

проводити регулярне (мінімум раз на тиждень) видалення непотрібних SMS-повідомлень, поштових повідомлень;

постійно перевіряти особистий МКП на предмет наявності ознак зламу та компрометації (*суттєве зниження працездатності, швидке розрядження, частий обрив з'єднань, зникнення власних коштів, періодична неочікувана поява небажаного контенту тощо*);

за необхідності передачі даних з МКП, особливо у випадку підключення до недовіреної (публічної) мережі Wi-Fi, використовувати програмні додатки для побудови віртуальної приватної мережі VPN (*Express VPN, Nord VPN, HotSpotShield, VPN Master тощо*) та програму-месенджер (*рекомендується Signal, WhatsApp та Threema*). Це дозволить підвищити захищеність інформації, яка передається, за рахунок шифрування даних (**Важливо:** передача інформації з обмеженим доступом при цьому заборонена);

використовувати складні паролі для доступу до облікових записів у онлайн-сервісах (електронних поштах, месенджерах тощо): пароль має бути випадковою послідовністю довжиною не менше 10 символів, містити літери великого та малого регістру, цифри та службові знаки, не містити доступної інформації про користувача та його найближчих родичів (*ім'я, прізвище, дата народження, телефон тощо*), та не містити частин логіну;

не передавати особисту інформацію, номери контактів інших осіб (без їх згоди), електронну поштову адресу, умовний ідентифікатор користувача месенджера особам, що не є довіреними;

використовувати окремі SIM-карти для особистого та службового користування; по можливості періодично їх міняти на нові;

періодично перевіряти налаштування МКП і програм, особливо після встановлення нової програми;

завжди відключати доступ до безпроводних мереж (Wi-Fi, Bluetooth, NFC), коли вони не потрібні, та вмикати його лише за реальної необхідності;

не підключатися до недовірених (публічних) Wi-Fi-мереж;

не здійснювати першу активацію SIM-карти МКП на території військових частин та об'єктів (у тому числі тимчасових);

у разі загрози отримання доступу до МКП сторонніми особами – терміново видалити всі дані з МКП:

для iOS – програма **Параметри** → **Загальні** → **Перенести дані чи скинути iPhone** → натиснути **Стерти весь зміст і параметри**. Якщо з'явиться запит на введення паролю – ввести пароль та підтвердити стирання;

для Android – програма **Налаштування** (іконка у вигляді коліщатка, що з'являється, після проведення по екрану згори донизу, або окрема іконка **Налаштування** на робочому екрані) → **Мій пристрій** (може мати назву **Про телефон**) → **Скидання налаштувань** → натиснути **Видалити всі дані** → Якщо з'явиться запит на введення паролю – ввести пароль та підтвердити стирання;

не встановлювати **непотрібні** програми та з **недовірених** джерел (довірені джерела – це офіційні онлайн-магазини програм: для Android – Google Play, для iOS – App Store). Під час завантаження нової програми на МКП перевірити надійність розробника та популярність додатка. Для цього подивитися відгуки та кількість завантажень;

при появі спливаючих вікон з пропозиціями перейти за посиланням або встановити програмне забезпечення – закривати їх не вчиняючи запропонованих дій;

не вводити персональні дані на запрошення програм без крайньої необхідності;

закривати програми коли закінчуєте роботу з ними:

для iOS – перейти на основний (домашній) екран → протягнути пальцем по екрану від нижнього краю угору, так, щоб з'явився стос вікон працюючих програм, → для закриття непотрібних програм по черзі зсунути їх вікна угору за межі екрану;

для Android – перейти на основний (домашній) екран → в нижньому краю екрану натиснути піктограму  (квадрат), так, щоб з'явилися зображення вікон працюючих програм, → для закриття непотрібних програм по черзі зсунути їх вікна вбік за межі екрану.

3. Рекомендації службі захисту інформації в автоматизованих системах для налаштування МКП.

Нижче зазначені налаштування проводяться силами служби захисту інформації в автоматизованих системах, відповідно до контрольного листа перевірки МКП на відповідність визначеним рекомендаціям щодо його кіберзахисту (додатки 2 та 3), та в присутності власника МКП.

3.1 Налаштування МКП для запобігання несанкціонованому доступу до нього:

В налаштуваннях операційної системи Android вимкнути режим “Налагодження USB”:

Налаштування → Додатково → Для розробників → Налагодження → USB-налагодження → обрати Вимкнути;

У разі наявності встановленого програмного забезпечення, що надає змогу віддаленого керування МКП, перевірити на наявність неідентифікованих активних сесій з невстановлених пристроїв. У разі наявності таких – видалити їх. встановити на SIM-карту пароль:

для iOS – програма Параметри → Стільникові дані → PIN-код → увімкнути перемикач PIN-код → у вікні, що з'явилося, надати можливість на введення PIN-коду SIM-карти власнику МКП → натиснути Готово;

для Android – програма Налаштування (іконка у вигляді коліщатка, що з'являється, якщо провести по екрану згори донизу, або окрема іконка Налаштування на робочому екрані) → Паролі та безпека → Конфіденційність → Блокування SIM-карти → вибрати SIM-карту → встановити перемикач в положення увімкнено → у вікні, що з'явилося, надати можливість на введення PIN-коду SIM-карти власнику МКП;

відключити автоматичний пошук мобільної мережі оператора зв'язку:

для iOS – програма Параметри → пункт Стільникові дані → пункт Вибір мережі → відключити функцію Автоматично → обрати з переліку мобільну мережу оператора виробника SIM-карти;

для Android – програма Налаштування → пункт SIM-карти та мобільні мережі → вибрати SIM-карту → пункт Мобільні мережі → відключити функцію Автоматично вибирати переважну мережу → обрати з переліку мобільну мережу оператора виробника SIM-карти;

відключити передачу даних з використанням мобільного інтернету:

для iOS – програма Параметри → Стільникові дані → встановити перемикач в положення вимкнено;

для Android – програма Налаштування → SIM-карти та мобільні мережі → Мобільний інтернет → встановити перемикач в положення вимкнено;

вимкнути точку роздачі Wi-Fi:

для iOS – програма Параметри → Стільникові дані → Власний хот-спот → встановити перемикач в положення вимкнено / (для старих версій iOS Параметри → Власний хот-спот → встановити перемикач в положення вимкнено);

для Android – програма Налаштування → Точка доступу Wi-Fi → Вимкнено;

налаштувати максимально безпечний порядок підключення до Wi-Fi мереж:

для iOS – запустити програму Параметри → Wi-Fi:

Питати про приєднання → обрати Вимкнено;

Хот-спот автоматом → обрати Ніколи;

здійснити підключення до довіреної мережі → натиснути знак ⓘ поруч із мережею → вимкнути перемикач **Автоприєднання** → також нижче за списком увімкнути перемикачі **Приватна адреса Wi-Fi** та **Обмеження відстеження за IP-адресою**;

для **Android** – програма **Налаштування** → **Wi-Fi** → у наданому переліку мереж обирати виключно довірену мережу → біля назви мережі натиснути стрілочку > → вимкнути **Підключатися автоматично**;

в розширених налаштуваннях Wi-Fi мереж провести видалення збережених Wi-Fi мереж, які не використовуються (особливо прихованих):

для **Android** – **Налаштування** → **Wi-Fi** → **Додаткові налаштування** → **Збережені мережі** → Видалити мережі, які не використовуються;

для **iOS** – **Параметри** → **Wi-Fi** → **Змінити** → обрати невідому/непотрібну мережу → натиснути **Видалити**;

налаштувати максимально безпечний порядок підключення Bluetooth:

для **iOS** – програма **Параметри** → **Bluetooth** → встановити перемикач в положення **Вимкнено**. Якщо є необхідність включити Bluetooth – після включення необхідно ретельно перевірити перелік доступних пристроїв, що з'явиться, та відключити невідомі та непотрібні пристрої: знайти у списку відповідний пристрій та натиснути знак ⓘ, → натиснути **Видалити цей пристрій**;

для **Android** – програма **Налаштування** → **Bluetooth** → встановити перемикач в положення **Вимкнено**. Якщо є необхідність включити Bluetooth – після включення необхідно ретельно перевірити перелік доступних пристроїв, що з'явиться, та відключити невідомі та непотрібні пристрої: біля назви пристрою натиснути стрілочку → вибрати пункт **Скасувати пару**;

налаштувати обмеження доступу до конфіденційної інформації:

для **iOS** – перейти у меню **Параметри** → **Приватність** → налаштувати доступ до кожної категорії інформації (**Контакти**, **Календарі тощо**), для чого натискати назву категорії та вимкати всі перемикачі для програм, яким недоцільно надавати доступ до цих категорій інформації;

для **Android** – програма **Налаштування** → **Конфіденційність** → налаштувати доступ до кожної категорії інформації, для чого натиснути назву категорії (**Сервіс автозаповнення від Google**, **Історія місцезнаходжень Google**, **Відстеження дій**, **Реклама**, **Використання та діагностика**) та вимкнути всі перемикачі для категорій яким недоцільно надавати доступ до інформації.

3.2 Налаштування для запобігання відстеженню геолокації:

відключити геолокацію:

для **iOS** – програма **Параметри** → **Приватність** → **Служби локації**:

встановити перемикач **Служби локації** в положення **вимкнено**;

Сигнали геопозиції → встановити перемикач **Карта в сигналах геопозиції** в положення **вимкнено**;

Моє місце (Локатор) → встановити перемикач **Поширювати геопозицію** в положення **вимкнено**; **Де iPhone** → встановити перемикач **Де iPhone** в положення **вимкнено**;

Приватність → Відстеження → Дозволити програмам надсилати запит на відстеження → встановити перемикач в положення вимкнено;

для Android – програма Налаштування → Конфіденційність → Історія місцезнаходжень Google → Відстеження дій → вибрати в налаштуваннях варіант вимкнено;

обов'язково вимкнути автоматичне присвоєння геоміток (інформації про розташування) до фотографій:

для iOS – програма Параметри → Приватність → Служби локації:

А) встановити перемикач Служби локації в положення вимкнено;

Б) якщо з якихось причин Служби локації мають бути включеними: → нижче у списку програм натиснути Камера → обрати Ніколи;

для Android – програма Налаштування → Програми → Системні програми → Камера → Зберегти місцезнаходження для фото → встановити перемикач в положення вимкнено;

видаляти інформацію про час та місце зйомки з фото- та відеофайлів (особливо при їх пересиланні):

для iOS – обрати потрібний файл або декілька файлів у Фотогалерії та:

А) натиснути значок ① → у вікні, що відкрилося, змінити (прибрати) час та місце зйомки;

або

Б) натиснути значок  → у вікні, що відкрилося, послідовно обрати пункти Коригувати дату й час та Змінити місце, та змінити (прибрати) значення дати, часу та місця зйомки. У цьому випадку інформація про час та місце зйомки буде видалена лише з файлу, який надсилається, та залишиться у вихідному файлі;

для Android – за замовчанням, відправлення зображень відбувається без даних про час та місце здійснення фотозйомки;

вимкнути персоналізацію реклами в операційній системі мобільного пристрою:

для iOS – перейти у меню Параметри → Приватність → Реклама від Apple → Персоналізована реклама → встановити перемикач в положення вимкнено;

для Android – програму Налаштування → Конфіденційність → Реклама → натиснути по черзі Скинути рекламний ідентифікатор та Видалити рекламний ідентифікатор та у вікнах, що з'являються, натиснути Підтвердити (Видалити...);

відключити сповіщення про ризик зараження Covid-19:

для iOS – перейти у меню Параметри → Сповіщення про контакт → перевірити, що Сповіщення про контактування та Оповістки про наявність вимкнено;

для Android – така функція відсутня, жодних дій не потрібно.

3.3. Налаштування для збереження конфіденційності даних на МКП:

налаштувати функцію видалення даних мобільного пристрою у разі 10 невдалих спроб автентифікації:

для iOS – перейти у меню **Параметри** → **Face ID і код допуску** або **Touch ID і код допуску** → увімкнути перемикач **Стерти дані**;

для Android – дана функція наразі недоступна.

При виконанні завдань у недовіреному середовищі або у безпосередній близькості до противника не використовувати технологій біометричної автентифікації для розблокування МКП (розпізнавання обличчя – Face ID, відбиток пальця – Fingerprint ID) (існують ризики можливості розблокування пристрою без згоди користувача, наприклад уві сні, при втраті свідомості або загибелі), натомість використовувати графічний ключ, PIN-код або пароль;

для вимкнення ідентифікації за обличчям:

для iOS – перейти у меню **Параметри** → **Face ID і код допуску** або **Touch ID і код допуску** → якщо перемикачі у розділі **Використовувати Face ID** увімкнені, натиснути **Скинути Face ID**;

для вимкнення ідентифікації за відбитком пальця – Fingerprint ID:

перейти у меню **Параметри** → **Touch ID і код допуску** в розділі **Touch ID і код допуску** вимкнути перемикач → **Відмикання iPhone, iTunes і App Store, Гаманець і Apple Pay**;

для Android – програма **Налаштування** → **Паролі та безпека** → **Блокування екрана** → **Змінити спосіб захисту** → вибрати варіант **Графічний ключ** або **PIN-код** або **Пароль**;

вимкнути голосовий помічник (Siri для iPhone, Google Асистент для Android, тощо):

для iOS – перейдіть у меню **Параметри** → **Siri і Пошук** → у розділі **Запити до Siri** переведіть тумблери **Чекати на “Привіт, Siri”** та **Тиснути бічну кнопку** у положення **вимкнено**, після чого з'явиться запитання з питанням, чи бажаєте ви повністю відключити **Siri**. Натисніть підтвердження **“Вимкнути Siri”**. Потім також деактивуйте всі перемикачі у розділах **Зміст від Apple** та **Пропозиції від Apple**. Далі відкрийте пункт **Історія Siri й Диктування** та натисніть **Видалити історію Siri й Диктування**;

для Android – програма **Налаштування** → **Програми** → **Дозволи** → **Дозволи** (підпункт має назву таку саму як пункт вищого рівня) → **Мікрофон** → **Google** → вибрати варіант **Заборонити** (або **Не дозволяти**);

налаштувати блокування екрану МКП через 1 хвилину бездіяльності (або менше):

для iOS – перейдіть у меню **Параметри** → **Дисплей і яскравість** → **Автозамикання** → Вибрати відповідний час бездіяльності до блокування;

для Android – запустити програму **Налаштування** → **Екран блокування** → **Режим “Сон”** → Вибрати мінімальний час бездіяльності до блокування;

вимкнути можливість попереднього перегляду сповіщень на МКП:

для iOS – перейдіть у меню **Параметри** → **Сповіщення**:

Звіт за розкладом → вимкнути перемикач **Звіт за розкладом**;

Передогляд → обрати **Ніколи**;

Поширення екрана → вимкнути перемикач **Дозволити сповіщення**;

Пропозиції Siri → вимкнути перемикач **Дозволити сповіщення**;

для Android – запустити програму **Налаштування** → **Екран блокування** → **Вмикати екран при отриманні сповіщень** → вимкнути дану функцію;

вимкнути автоматичну синхронізацію із сервісами зберігання даних iCloud, GoogleDisk, тощо;

для iOS – перейти у меню **Параметри** та натисніть на логін, після чого виберіть **iCloud** та вимкніть всі перемикачі для всіх програм;

для Android – запустити програму **Налаштування** → **Акаунти та синхронізація** → **Автосинхронізація даних** → вимкнути дану функцію;

вимкнути збір та передачу інформації про мобільний пристрій та збоїв у роботі;

для iOS – перейти у меню **Параметри** → **Приватність** → **Аналітика і Вдосконалення** вимкнути **Поширювати аналітику iPhone**;

для Android – запустити програму **Налаштування** → **Конфіденційність** → **Використання та діагностика** → Вибрати варіант **Вимкнено**.

3.4. Налаштування месенджерів

На спеціально налаштовані МКП заборонено встановлювати будь-які месенджери, окрім Signal, WhatsApp та Threema.

3.4.1 Налаштування месенджера Signal:

при створенні профілю не використовувати власне актуальне фотозображення та не вказувати справжні персональні дані;

активувати функцію додаткового захисту доступу до месенджеру шляхом введення PIN-коду, для цього:

для iOS – натиснути в лівому верхньому куті екрану **пiktogramу облікового запису** → вибрати пункт **Налаштування** → **Обліковий запис** → **Створіть PIN-код**;

для Android – натиснути в лівому верхньому куті екрану **пiktogramу облікового запису** для переходу в меню **Налаштування** → вибрати пункт **Обліковий запис** → **Створіть PIN-код**;

заблокувати можливість реєстрації номеру телефону в месенджері без введення PIN-коду (для запобігання “угону” облікового запису):

для iOS – натиснути в лівому верхньому куті екрану **пiktogramу облікового запису** → вибрати пункт **Налаштування** → **Обліковий запис** → встановити перемикач **Блокування реєстрації** в положення **увімкнено**;

для Android – натиснути в лівому верхньому куті екрану **пiktogramу облікового запису** → вибрати пункт **Обліковий запис** → встановити перемикач **Блокування доступу** в положення **увімкнено**;

перевірити та видалити прив’язані пристрої, які невідомі або відомі, проте не використовуються у цей час. Для цього:

для iOS – натиснути в лівому верхньому куті екрану **пiktogramу облікового запису** → вибрати пункт **Налаштування** → **Прив’язані пристрої** → в правому верхньому куті екрану **Змінити** → у переліку пристроїв, що висвітився, обрати пристрій, який потрібно відв’язати;

для Android – натиснути в лівому верхньому куті екрану **пiktogramу облікового запису** → **Прив’язані пристрої** → у переліку пристроїв,

що висвітлюється, обрати пристрій, який потрібно від'єднати, натиснути на його назву → у діалоговому вікні обрати варіант **Ок**;

заблокувати відображення змісту отриманих сповіщень на екрані МКП:

для iOS – натиснути в лівому верхньому куті екрану **пінтограму облікового запису** → вибрати пункт **Налаштування** → **Сповіщення** → **Вміст сповіщень** → увімкнути опцію **Лише ім'я** або **Без імені чи вмісту**;

для Android – натиснути в лівому верхньому куті екрану **пінтограму облікового запису** → **Сповіщення** → **Показувати** → увімкнути опцію **Тільки ім'я** або **Немає імені чи повідомлення**;

обмежити час зберігання даних в чатах (листування, фото/відео, тощо) мінімальним терміном, для цього:

для iOS – натиснути в лівому верхньому куті екрану **пінтограму облікового запису** → вибрати пункт **Налаштування** → **Конфіденційність (Приватність)** → **Таймер за замовчуванням для нових чатів** → обрати мінімальний зручний час, рекомендовано – не більше 1 тижня;

зайти по черзі в існуючі чати → натиснути в лівому верхньому куті екрану **пінтограму чату** (групи або контакту) → вибрати пункт **Зникаючі повідомлення** → мінімальний зручний час, рекомендовано – не більше 1 тижня;

для Android – натиснути в лівому верхньому куті екрану **пінтограму облікового запису** → **Приватність** → **Таймер за умовчанням для нових чатів** → обрати мінімальний зручний час, рекомендовано – не більше 1 тижня;

зайти по черзі в існуючі чати → натиснути в лівому верхньому куті екрану **пінтограму чату** (групи або контакту) → вибрати пункт **Зникаючі повідомлення** → мінімальний зручний час, рекомендовано – не більше 1 тижня;

встановити мінімальний час блокування доступу до месенджера, для цього:

для iOS та Android перейти у меню **Налаштування** → **Конфіденційність (Приватність)** та:

поставити перемикачі **Приховувати екран у перемикачі застосунків** та **Блокування екрану в положення увімкнено**;

торкнутися пункту **Затримка блокування екрану** → обрати мінімальний зручний час, рекомендовано 1 хвилина);

увімкнути заборону видимості у мережі:

для iOS – натиснути в лівому верхньому куті екрану **пінтограму облікового запису** → вибрати пункт **Налаштування** → **Конфіденційність** → **Додаткові функції** → встановити:

перемикач **Завжди ретранслювати дзвінки** в положення увімкнено;

перемикачі **Показувати іконку стану** та **Дозволити від усіх** в положення вимкнено;

для Android – натиснути в лівому верхньому куті екрану **пінтограму облікового запису** для переходу в меню **Налаштування** → **Приватність** → **Розширені** → встановити перемикач **Показати значок статусу** в положення вимкнено;

обмежити дозволи для членів груп, які адмініструються власником МКП:

для iOS – зайти по черзі в групи, які адмініструються власником МКП → натиснути в лівому верхньому куті екрану **піктограму групи**, далі:

вибрати пункт **Посилання групи** → встановити перемикач **Затвердити нових учасників в положення увімкнено**;

вибрати пункт **Дозволи** → у пунктах **Додати учасників та Редагувати інформацію про групу** обрати пункти **Тільки адміністратори**;

для Android – зайти по черзі в групи, які адмініструються власником МКП → натиснути в лівому верхньому куті екрану **піктограму групи**, далі:

вибрати пункт **Посилання групи** → встановити перемикач в положення **Увімкнено** → **Схвалити нові запити в положення увімкнено**;

вибрати пункт **Дозволи** → у пункті **Додати учасників та Редагувати інформацію про групу** обрати пункти **Тільки адміністратори**;

по можливості, підтвердьте особи контактів в чатах:

для iOS – зайти по черзі в чати → натиснути в лівому верхньому куті екрану **піктограму контакту** → вибрати пункт **Подивитись код безпеки** → разом з Вашим кореспондентом виконайте дії, описані у вікні, що з'явиться;

для Android – зайти по черзі в чати → натиснути в лівому верхньому куті екрану **піктограму контакту** → вибрати пункт **Перевірити номер безпеки** → разом з Вашим кореспондентом виконайте дії, описані у вікні, що з'явиться.

У разі якщо налаштування групи, членом якої є користувач, не відповідає зазначеним вимогам, зв'язатися з визначеним адміністратором цієї групи та застосувати зазначені налаштування. У разі виникнення проблемних питань – з службою захисту інформації в автоматизованих системах чи з черговою зміною ЦБІ військової частини А0334.

3.4.2 Налаштування месенджера WhatsApp:

при створенні свого профілю не використовувати актуальне фотозображення та не вказувати справжні персональні дані;

активувати функцію двоетапної перевірки, для цього:

натиснути на піктограму **Параметри** (для iOS – зображення шестерні, для Android – три крапки) → **Обліковий запис** → **Двоетапна перевірка** → натиснути на **Увімкнути** → надати можливість створити 6-значний PIN-код власнику МКП, який власник МКП зможе запам'ятати;

налаштувати параметри конфіденційності облікового запису, для цього:

натиснути на піктограму **Параметри** (для iOS – зображення шестерні, для Android – три крапки) → **Конфіденційність** → та налаштувати наступні параметри:

→ **Хто може бачити мій статус “Востаннє в мережі”** → **Мої контакти**

→ **Хто може бачити, коли я в мережі** → **Ті ж користувачі, які бачать “Востаннє в мережі”**

→ **Востаннє в мережі** → **Мої контакти**

→ **Фото профілю** → **Мої контакти**

→ **Звістка** → **Мої контакти**

→ **Статус** → **Мої контакти**

→ *Групи* → *Мої контакти*

→ *Геодані* → *Немає*

налаштувати заборону автозавантаження медіафайлів:

натиснути на піктограму Параметри (для iOS – зображення шестерні, для Android – три крапки) → Сховище й дані → у області Автозавантаження медіафайлів обрати значення Ніколи для кожного з параметрів

у групах, які адмініструються власником МКП налаштуйте можливість на додавання нових учасників лише адміністратором групи, а також на схвалення нових учасників групи лише адміністратором.

У разі якщо налаштування групи, членом якої є користувач, не відповідає зазначеним вимогам, зв'язатися з визначеним адміністратором цієї групи та застосувати зазначені налаштування. У разі виникнення проблемних питань – з службою захисту інформації в автоматизованих системах чи з черговою зміною ЦБІ військової частини А0334.

3.4.3 Налаштування месенджера Threema:

при створенні свого профілю не використовувати актуальне фотозображення, не вказувати справжні персональні дані, не прив'язувати обліковий запис до номеру мобільного телефона та виключити резервне копіювання Threema Safe, яке зберігає дані на серверах компанії Threema GmbH;

активувати функцію додаткового захисту доступу до месенджера шляхом введення паролю, для цього:

для iOS – натиснути в правому нижньому куті екрану Налаштування → Блокування за допомогою пароля → Увімкнути введення пароля;

для Android – натиснути в лівому верхньому куті екрану три крапки для переходу в меню Налаштування → вибрати пункт Безпека → Механізм блокування → обрати пункт Пін-код або пароль;

перевірити та видалити прив'язані пристрої, які невідомі або відомі, проте не використовуються у цей час. Для цього:

для iOS – натиснути в правому нижньому куті екрану Налаштування → Застосунок/Вебверсія → Прив'язаний пристрій → у переліку пристроїв, що висвітився, обрати пристрій, який потрібно від'єднати, натиснути на його назву → у діалоговому вікні обрати варіант Ок;

для Android – натиснути в лівому верхньому куті екрану три крапки для переходу в меню Застосунок/Вебверсія, у переліку пристроїв, що висвітився, обрати пристрій, який потрібно від'єднати, натиснути на його назву → у діалоговому вікні обрати варіант Ок;

заблокувати відображення змісту отриманих сповіщень на екрані МКП:

для iOS – натиснути в правому нижньому куті екрану Налаштування → Сповіщення → у секціях У застосунку та Push-сповіщення вимикаємо перемикач Попередній перегляд повідомлення;

для Android – натиснути в лівому верхньому куті екрану три крапки для переходу в меню Налаштування → Звук і сповіщення, прогорнути до низу екрану та вимикаємо перемикач Попередній перегляд повідомлення;

встановити мінімальний час блокування доступу до месенджера, для цього:

для iOS – натиснути в правому нижньому куті екрану **Налаштування** → **Блокування за допомогою пароля** → **Вимагати пароль** та обрати мінімальний зручний час (рекомендовано 1 хвилина);

для Android – натиснути в лівому верхньому куті екрану **три крапки** для переходу в меню **Налаштування** → вибрати пункт **Безпека** → **Час блокування пароль** та обрати мінімальний зручний час (рекомендовано 1 хвилина);

увімкнути ретрансляцію викликів:

для iOS – натиснути в правому нижньому куті екрану **Налаштування** → **Виклики Threema** → встановити перемикач **Завжди ретранслювати виклики** в положення **увімкнено**;

для Android – натиснути в лівому верхньому куті екрану **три крапки** для переходу в меню **Налаштування** → вибрати пункт **Дзвінки (Виклики)** → встановити перемикач **Завжди ретранслювати виклики** в положення **увімкнено**;

по можливості, підтвердьте особи контактів в діалогах:

для iOS – зайти по черзі в діалоги → натиснути на **піктограму контакту** → вибрати пункт **Рівень підтвердження** → разом з кореспондентом виконайте дії, описані у вікні, що з'явиться;

для Android – зайти по черзі в діалоги → натиснути на **піктограму контакту** → натиснути на іконку **Інформація** → разом з кореспондентом виконайте дії, описані у вікні, що з'явиться.

У разі якщо налаштування групи, членом якої є користувач, не відповідає зазначеним вимогам, зв'язатися з визначеним адміністратором цієї групи та застосувати зазначені налаштування. У разі виникнення проблемних питань – з службою захисту інформації в автоматизованих системах чи з черговою зміною ЦБІ військової частини А0334.

3.5. Налаштування для безпечного користування застосунками (програмами, додатками):

вимкнути можливість встановлення програмних додатків з невідомих джерел:

для iOS – здійснювати встановлення програмних додатків лише з офіційної платформи “App Store”, інші сторонні програмні додатки з невідомих джерел автоматично блокуються операційною системою пристрою;

для Android – запустити програму **Налаштування** → **Захист конфіденційності** → **Особливі сповіщення** → **Встановити невідомі програми** → Відкриється перелік додатків, для кожного необхідно обрати варіант **Заборонено**;

періодично перевіряти перелік встановлених програм і частоту їх використання. Видалити всі програми, які не встановлювалися, та ті, що не потрібні, а також такі, що неконтрольовано збирають та розповсюджують дані з МКП (наприклад – Getcontact);

перевіряти наявність оновлень для операційної системи та встановлених додатків:

для *Android* – відкрити додаток *PlayMarket* → перейти в обліковий запис, натиснувши піктограму облікового запису у правому верхньому куті → натиснути пункт меню *Керування: додатки й пристрій* → в пункті меню *Оновлення додатків* → натиснути *Оновити всі*;

для *iOS* – відкрити додаток *AppStore* → перейти в обліковий запис, натиснувши піктограму облікового запису у правому верхньому куті → в пункті меню *Доступні оновлення* → натиснути *Оновити всі*;

здійснювати очищення пам'яті МКП та кешу, встановлених додатків:

Налаштування → *Програми* → *Всі програми* → *Вибрати програму* → *Сховище* → *Очистити дані* → *Очистити кеш*

не використовувати російські програмні продукти, соціальні мережі, месенджери (*Viber, Telegram, MapsMe, 2gis, Getcontact* тощо);

здійснити налаштування дозволів щодо використання програмами різних функцій та фізичних модулів (мікрофон, камера, Wi-Fi модуль тощо):

для *iOS* – перейти у меню *Параметри* → *Приватність (Конфіденційність)* → послідовно натиснути кожну функцію у переліку (*Контакти, Календарі, Нагадування, Фотографії, Bluetooth, Локальна мережа, взаємодія поблизу, Мікрофон, Розпізнавання мовлення, Камера, тощо*) та у вікнах, що з'являються, відключити доступ до зазначених функцій тим програмам зі списку, яким він не потрібен. Для цього перевести відповідні перемикачі у положення *вимкнено*.

Після цього повернутися в меню *Параметри* та послідовно натиснути кожну програму у переліку (*App Store, Гаманець і Apple Pay, Паролі, Пошта, Контакти, Календар, Нотатки, Нагадування, Диктофон, Телефон, Повідомлення, тощо*) та у вікнах, що з'являються, для кожної програми зі списку відключити доступ до функцій, які передбачають передачу геолокації, збір та передачу персональної інформації, доступ до контактів, камери, мікрофону, фотографій, файлів та тек;

для *Android* – перейдіть у меню *Налаштування* → *Захист конфіденційності (Конфіденційність)* → *Конфіденційні дії* (може мати назву *Диспетчер дозволів*) → послідовно натиснути кожен тип дозволу у переліку (*Геодані, Датчики на тілі, Журнали викликів, Календар, Камера, Контакти, Мікрофон, Телефон, Файли й мультимедіа, Фізична активність, SMS, додаткові дозволи тощо*) та у вікнах, що з'являються, відключити доступ до зазначених функцій тим програмам зі списку, яким він не потрібен. Для цього активувати відповідні пункти *Дозволити, Заборонити, Дозволяти, лише коли додаток використовується, Запитувати кожного разу тощо*.

Після цього повернутися в меню *Налаштування* → *Програми* → *Всі програми* → послідовно натиснути кожну програму у переліку (*Безпека, Галерея, Засоби SIM, Інтерфейс системи, Камера, Налаштування, Повідомлення, Пошук пристрою, Робочий стіл, Телефонні служби, Bluetooth тощо*) та у вікнах, що з'являються, вибрати пункт *Дозволи програм* й по списку, який відобразиться, перевірити доступ до функцій, які передбачають передачу

геолокації, збір та передачу персональної інформації, доступ до контактів, камери, мікрофону, фотографії, файлів та тек.

Начальник Головного управління зв'язку та кібербезпеки
Генерального штабу Збройних Сил України
генерал-майор



Віктор ОСТАПЧУК

Додаток 2
До Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами (пункт 3 додатку 1)

КОНТРОЛЬНИЙ ЛИСТ
перевірки мобільного комунікаційного пристрою на відповідність
визначеним рекомендаціям щодо його кіберзахисту

(найменування військової організаційної структури)

Назва структурного підрозділу, № приміщення	Військове звання, прізвище ім'я та по батькові власника засобу мобільного комунікаційного пристрою (МКП)	Назва моделі та заводський (інвентарний) номер (версія ОС) МКП	IP-адреса (за потреби), MAC-адреса

Алгоритм дій

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
1.	Поінформувати власника МКП, що подальші дії з МКП проводяться задля підвищення захищеності МКП та даних, які на ньому зберігаються, проводяться у присутності власника та за його згодою у разі її отримання. Отримати згоду власника на проведення наступних пунктів Алгоритму перевірки (усіх або деяких з них). У разі відмови власника щодо виконання окремих пунктів, робити помітку в графі "Примітка" навпроти цих пунктів	☐	
2.	Змінити раніше встановлений власником МКП пароль доступу на тимчасовий та вказати пароль у полі "Примітка" Алгоритму перевірки <i>Налаштування → Паролі та безпека → Блокування екрану → PIN-код</i>	☐	
3.	Опитати власника про наявність підозрілих SMS-повідомлень, поштових та інших повідомлень (із сумнівними/фішинговими посиланнями) або іншої аномальної активності. У випадку підтвердження власником МКП отримання таких повідомлень за його згодою здійснити пошук та їх виявлення, після чого переслати їх на поштову скриньку csoc@post.mil.gov.ua або відповідний номер чергової зміни ЦКБ військової частини А0334 в Signal з метою подальшого аналізу. Після чого видалити виявлені повідомлення.	☐	
4.	За згодою власника МКП тимчасово перевести мову пристрою на українську (якщо мова менш, наприклад, англійська) для зручного здійснення подальших налаштувань <i>Налаштування → Додатково → Мова та введення → Мови</i>	☐	
5.	Здійснити перезавантаження МКП	☐	
6.	Встановити на SIM-карти паролі, при цьому попросити власника їх ввести та записати собі за наявності доступу до GSM мережі: <i>Налаштування → Паролі та безпека → Конфіденційність → Мобільний оператор → Блокування SIM карти → Змінити PIN-код</i> за відсутності доступу до GSM мережі – надати рекомендації та порядок встановлення паролю на SIM-карти для здійснення налаштування при появі доступу до GSM мережі.	☐	
7.	Відключити автоматичний пошук мобільної мережі оператора стільникового зв'язку <i>Налаштування → SIM-картки та мобільні мережі → Мобільні мережі → Обрати кожну мережу → Автоматично вибирати мережу</i>	☐	
8.	Вимкнути точку роздачі Wi-Fi (власний хот-спот) <i>Налаштування → Підключення та загальний доступ → Точка доступу Wi-Fi → Обрати вимкнути</i>	☐	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
9.	В розширених налаштуваннях Wi-Fi мереж провести видалення збережених Wi-Fi мереж, які не використовуються (особливо прихованих) <i>Налаштування → Wi-Fi → Додаткові налаштування → Збережені мережі → Видалити мережі, які не використовуються</i>	☐	
10.	Вимкнути автоприєднання до мереж Wi-Fi <i>Налаштування → Wi-Fi → Обрати довірену мережу → В деталях мережі вимкнути можливість підключатися автоматично</i>	☐	
11.	Налаштувати максимально безпечний порядок підключення Bluetooth (ретельно перевірити перелік доступних пристроїв та відключити невідомі та непотрібні пристрої) <i>Налаштування → Bluetooth → встановити перемикач в положення Включено. Після включення необхідно ретельно перевірити перелік доступних пристроїв, що з'являться, та відключити невідомі та непотрібні пристрої: знайти у списку відповідний пристрій → Обрати скасувати пару</i>	☐	
12.	В налаштуванні параметрів МКП (Дисплей та яскравість) налаштувати блокування екрану МКП через 1 хвилину бездіяльності <i>Налаштування → Активний екран та блокування → Режим "Сон" → обрати 1 хвилину</i>	☐	
13.	В налаштуванні параметрів МКП (Сповіщення) вимкнути можливість попереднього перегляду сповіщень на екрані МКП <i>Налаштування → Активний екран та блокування → Завжди активний екран → встановити перемикач в положення Вимкнено</i> <i>Налаштування → Активний екран та блокування → Сповіщення на вимкненому екрані → обрати Немає</i>	☐	
14.	В налаштуваннях операційної системи android активізувати опцію заборони встановлення невідомих програм та відключити режим "Налагодження USB" <i>Налаштування → Додатково → Для розробників → Налагодження → USB-налагодження</i> <i>Налаштування → Конфіденційність → Керувати → Спеціальний доступ → Встановити невідомі програми → Заборонено</i>	☐	
15.	В налаштуванні параметрів МКП вимкнути голосовий помічник (Google Асистент для Android) <i>Налаштування → Додатково → Функції кнопок → Запустити Google помічник → Обрати Немає</i>	☐	
16.	Перевірити МКП на наявність встановлення підозрілих додатків та додатків соціальних мереж та месенджерів, роботу яких пов'язують із російською федерацією (VK.com, Однокласники, Mail.ru, Яндекс Карти, Яндекс Перекладач, Яндекс Браузер, Яндекс Пошта, Яндекс Диск, IVI, MapsMe, 2gis, Getcontact, ДМБ таймер, FaceApp, NewProfilePic, Dr. Web, LinguaLeo, Kaspersky Secure Connection і т.п.), в разі виявлення – видалити. Опитати власника МКП на рахунок доцільності використання ним додатків, що мало використовуються (мають обмежений, безкорисний функціонал) та видалити такі додатки за згодою власника МКП <i>Налаштування → Програми → Керування програмами → Видалити → Обрати відповідні програми</i>	☐	
17.	Перевірити на наявність у календарі пристрою (також за наявності Google Календар) запрошень, свят та інших заходів які власником пристрою не були додані чи заплановані. За згодою власника видалити такі заходи та попередити про недопущення згоди на використання календарю сторонніми програмами (додатками). <i>Налаштування → Програми → Системні програми → Календар → Акаунти календаря → Обрати всі</i> <i>Календар(програма) → Події → Видалити не створені користувачем</i> <i>Налаштування → Програми → Календар → Сховище → Очистити дані</i>	☐	
18.	Здійснити очищення пам'яті МКП та кешу, встановлених додатків на МКП <i>Налаштування → Програми → Всі програми → Вибрати програму → Сховище → Очистити дані → Очистити кеш</i>	☐	
19.	Оновити встановлені на МКП додатки до останньої доступної версії та активувати функцію їх автооновлення <i>Налаштування → Оновлення системних програм → Оновити все</i> <i>Налаштування → Статус захисту → Оновлення безпеки</i> <i>Налаштування → Програми → Системні програми → Оновлення системних програм</i>	☐	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	<i>Play Market → У верхньому правому куті обрати зображення облікового запису → Керування: додатки і пристрій → Доступні оновлення → оновити всі</i>		
20.	Налаштувати максимальне обмеження доступу до конфіденційної інформації (геолокації, стільникових даних, фото галереї, веб-камери, контактів, мікрофону та інше) для кожного встановленого на МКП додатку в залежності від потреби його власника <i>Запит на дозвіл має відповідати мінімально необхідному функціоналу програми, а також враховувати міркування безпеки.</i> <i>Наприклад: застосунок з географічними даними може мати доступ до даних геолокацій, а якщо програма просить доступ до контактів, галереї, право вносити зміни до пристрою тощо, це вже має бути заборонено.</i> <i>Налаштування → Програми → Всі програмами → Дозволи → Заборонити відповідний дозвіл до вказаних додатків</i>	☐	
21.	В налаштуваннях МКП відключити дозволи програмам, які не передбачені функціоналом цих програм <i>Запит на дозвіл має відповідати мінімально необхідному функціоналу програми, а також враховувати міркування безпеки.</i> <i>Наприклад: застосунок з географічними даними може мати доступ до даних геолокацій, а якщо програма просить доступ до контактів, галереї, право вносити зміни до пристрою тощо, це вже має бути заборонено.</i> <i>Налаштування → Програми → Дозволи → Обрати відповідний функціонал пристрою → Обрати програму для якої планується обмеження доступу → Заборонити доступ для цього додатку</i>	☐	
22.	В налаштуваннях МКП відключити служби локації (доступ до місцезнаходження, доступ додатка до геоданих, доступ камери до геоданих та інше) <i>Налаштування → Місцезнаходження → Доступ додатка до даних → Камера (також ті додатки для функціональності яких не потрібно мати доступ до геоданих) → Заборонити доступ до геоданих для цього додатка</i> <i>Налаштування → Місцезнаходження → Пошук Wi-Fi та Bluetooth → Шукати мережі Wi-Fi → встановити перемикач в положення Вимкнено → Шукати пристрої Bluetooth → встановити перемикач в положення Вимкнено</i> <i>Налаштування → Місцезнаходження → Доступ до місцезнаходження → встановити перемикач в положення Вимкнено</i>	☐	
23.	В налаштуваннях МКП (в налаштуваннях приватності) вимкнути персоналізацію реклами в операційній системі мобільного пристрою <i>Налаштування → Пароль та безпека → Конфіденційність → Програма поліпшення якості встановити перемикач в положення Вимкнено</i> <i>Налаштування → Пароль та безпека → Конфіденційність → Рекламні сервіси → Персональна реклама встановити перемикач в положення Вимкнено</i>	☐	
24.	В налаштуваннях МКП видалити рекламний ідентифікатор пристрою: <i>Налаштування → Конфіденційність → Реклама → натиснути по черзі Скинути рекламний ідентифікатор та Видалити рекламний ідентифікатор та у вікнах, що з'являються, натиснути Підтвердити (Видалити...)</i>	☐	
25.	В налаштуванні параметрів МКП (в налаштуваннях приватності) вимкнути збір та передачу інформації про мобільний пристрій та збої у роботі <i>Налаштування → Пароль та безпека → Конфіденційність → Надсилати діагностичні дані автоматично встановити перемикач в положення Вимкнено</i>	☐	
26.	В разі необхідності використання власником месенджера Signal, в налаштуваннях Signal необхідно: активувати функцію додаткового захисту доступу до месенджера шляхом введення PIN-коду або використання біометричної автентифікації (сканування обличчя або відбитків пальця) <i>Signal → Обліковий запис → Pin Signal</i> заблокувати можливість ресстрації номеру телефону в месенджері без введення PIN-коду <i>Signal → Обліковий запис → Pin Signal</i> обмежити час зберігання даних в чатах (листування, фото/відео, тощо) мінімальним терміном (за погодженням з власником) <i>Signal → Розмова → налаштування розмови → Зникаючі повідомлення увімкнути заборону видимості у мережі</i>	☐	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	натиснути в лівому верхньому куті екрану піктограму облікового запису → вибрати пункт Налаштування → Конфіденційність → Додаткові функції → встановити перемикач Завжди ретранслювати дзвінки в положення Включено; перемикачі Показувати іконку стану та Дозволити від усіх в положення вимкнено обмежити дозволи для членів груп, які адмініструє власник МКП зайти по черзі в групи, які ви адмініструєте → натиснути в лівому верхньому куті екрану піктограму групи, далі: вибрати пункт Посилання групи → увімкнути групове посилання → встановити перемикач Затвердити нових учасників в положення Вимкнено; вибрати пункт Дозволи → у пунктах Додати учасників та Редагувати інформацію про групу обрати пункти Тільки адміністратори заборонити можливість робити знімки екрану Налаштування → Приватність → Безпека екрану. Блокувати знімки екрану в списку недавніх та в програмі видалити невідомі або які не використовуються прив'язані пристрої Налаштування → Прив'язані пристрої → Вибрати пристрій та від'єднати його		
27.	В разі встановлення на МКП інших месенджерів, які у своїх налаштуваннях, окрім згаданого в пункті 11, дозволяють заборонити відображення мобільного номера користувача, вимкнути геолокацію, збір аналітики (у тому числі засобами віртуальної клавіатури), персоналізацію контенту, та налаштування інших параметрів безпеки – все заборонити (відключити), увімкнути двоетапну перевірку (двофакторну автентифікацію), а також перевірити та видалити прив'язані пристрої в налаштуваннях аккаунтів, які невідомі або відомі власнику МКП, проте не використовуються Google Обліковий запис → Налаштування → Дані й конфіденційність → Історія місцезнаходження → Призупинено Обліковий запис → Налаштування → Дані й конфіденційність → Інформація, якою ви можете ділитися з іншими → → Профіль → Ім'я → Будь-хто → Зображення → Лише ви → Стат'я → Лише ви → Дата народження → Лише ви → Електронна адреса → Будь-хто Обліковий запис → Налаштування → Дані й конфіденційність → Інформація, якою ви можете ділитися з іншими → Надсилання геоданих → Ви нікому не надсилаєте свої геодані Обліковий запис → Безпека → → Двоетапна перевірка → Увімкнути → Номер телефону для відновлення → Ввести номер → Резервна електронна адреса → Ввести адресу → Керувати всіма пристроями → Завершити прив'язані пристрої, які не відомі користувачу → Керувати доступом сторонніх додатків → Обрати додаток → Скасувати доступ → Менеджер паролів → Видалити непотрібні паролі WhatsApp Налаштування → Обліковий запис → Двоетапна перевірка → Увімкнути Налаштування → Конфіденційність → → Хто може бачити мій статус "Востаннє в мережі" → Мої контакти → Хто може бачити, коли я в мережі → Ті ж користувачі, які бачать "Востаннє в мережі" → Востаннє в мережі → Мої контакти → Фото профілю → Мої контакти → Звістка → Мої контакти → Статус → Мої контакти → Групи → Мої контакти → Геодані → Немає Threema	□	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	Натиснути в лівому верхньому куті екрану три крапки для переходу в меню Налаштування → вибрати пункт Безпека → Механізм блокування → обрати пункт Пін-код або пароль; натиснути в лівому верхньому куті екрану три крапки для переходу в меню Застосунок/Вебверсія, у переліку пристроїв, що висвітився, обрати пристрій, який потрібно від'єднати, натиснути на його назву → у діалоговому вікні обрати варіант Ок; натиснути в лівому верхньому куті екрану три крапки для переходу в меню Налаштування → Звук і сповіщення, прогорнути до низу екрану та вимикаємо перемикач Попередній перегляд повідомлення; натиснути в лівому верхньому куті екрану три крапки для переходу в меню Налаштування → вибрати пункт Безпека → Час блокування пароль та обрати мінімальний зручний час (рекомендовано 1 хвилина); натиснути в лівому верхньому куті екрану три крапки для переходу в меню Налаштування → вибрати пункт Дзвінки (Виклики) → встановити перемикач Завжди ретранслювати виклики в положення увімкнено; зайти по черзі в діалоги → натиснути на піктограму контакту → натиснути на іконку Інформація → разом з кореспондентом виконайте дії, описані у вікні, що з'явиться.		
28.	Змінити мову меню пристрою на раніше обрану (якщо мова змінювалася для проведення налаштувань)	☐	
29.	Забезпечити зміну паролю доступу до МКП його власником	☐	
30.	Здійснити перезавантаження МКП	☐	
31.	Встановити останнє доступне оновлення для операційної системи, встановленої на МКП та активувати функцію автооновлення (після перезавантаження) Налаштування → Про телефон → Версія MIUI → Перевірити оновлення	☐	
32.	Нагадати власнику МКП про необхідність відключати безпроводні мережі (Wi-Fi, Bluetooth, NFC, AirDrop), коли їх робота не потрібна, та перезавантажувати МКП щонайрідше раз на тиждень, краще – щоденно.	☐	

(посада, військове звання, підпис, ім'я та прізвище особи, що здійснювала перевірку)

Додаток 3
До Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами (пункт 3 додатку 1)

КОНТРОЛЬНИЙ ЛИСТ
перевірки мобільного комунікаційного пристрою на відповідність
визначеним рекомендаціям щодо його кіберзахисту

(найменування військової організаційної структури)

Назва структурного підрозділу, № приміщення	Військове звання, прізвище ім'я та по батькові власника засобу мобільного комунікаційного пристрою (МКП)	Назва моделі, версія ОС та заводський (інвентарний) номер МКП	ІР-адреса (за потреби), MAC-адреса

Алгоритм перевірки

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
1.	Поінформувати власника МКП, що подальші дії з МКП проводяться задля підвищення захищеності МКП та даних, які на ньому зберігаються, проводяться у присутності власника та за його згодою у разі її отримання. Отримати згоду власника на проведення наступних пунктів Алгоритму перевірки (усіх або деяких з них). У разі відмови власника щодо виконання окремих пунктів, робити помітку в графі "Примітка" навпроти цих пунктів	☐	
2.	Змінити раніше встановлений власником МКП пароль доступу на тимчасовий та вказати пароль у полі "Примітка" Алгоритму перевірки (навпроти цього пункту) <i>Параметри → Face ID і код доступу → Змінити код допуску → вказати новий код → підтвердити введений код</i>	☐	
3.	Опитати власника про наявність підозрілих SMS-повідомлень, поштових та інших повідомлень (із сумнівними/фішинговими посиланнями) або іншої аномальної активності. У випадку підтвердження власником МКП отримання таких повідомлень за його згодою здійснити пошук та їх виявлення, після чого переслати їх на поштову скриньку csoc@post.mil.gov.ua або відповідний номер чергової зміни ЦКБ військової частини А0334 в Signal з метою подальшого аналізу. Після чого видалити виявленні повідомлення.	☐	
4.	За згодою власника МКП тимчасово перевести мову пристрою на українську (якщо мова меню, наприклад, англійська) для зручного здійснення подальших налаштувань	☐	
5.	Здійснити перезавантаження МКП <i>Одноразове затискання протягом деякого часу клавіші збільшення/зменшення гучності та блокування телефону</i>	☐	
6.	Встановити на SIM-карту пін-коди достатньої складності, при цьому попросити власника їх ввести та записати собі за наявності доступу до GSM мережі: <i>Параметри → Стільникові дані → PIN-код → активувати функцію увімкнувши перемикач → Встановити PIN-код та натиснути "Готово"</i> за відсутності доступу до GSM мережі – надати рекомендації та порядок встановлення паролю на SIM-карти для здійснення налаштування при появі доступу до GSM мережі.	☐	
7.	Відключити автоматичний пошук мобільної мережі оператора стільникового зв'язку <i>Параметри → Стільникові дані → Вибір мережі → відключити функцію Автоматично → обрати з переліку мобільну мережу свого оператора</i>	☐	
8.	Вимкнути точку роздачі Wi-Fi (власний хот-спот)	☐	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	<i>Параметри → Стільникові дані → Власний хот-спот → встановити перемикач в положення вимкнено (для старих версій iOS: Параметри → Власний хот-спот → встановити перемикач в положення вимкнено)</i>		
9.	В розширених налаштуваннях Wi-Fi мереж провести видалення збережених Wi-Fi мереж, які не використовуються (особливо прихованих) <i>Параметри → Wi-Fi → змінити → видалити зайві</i>	☐	
10.	Налаштувати максимально безпечний порядок підключення до Wi-Fi мереж: вимкнути функцію “Хот-спот автоматом” <i>Параметри → Wi-Fi:</i> <i>Хот-спот автоматом → обрати Ніколи;</i> вимкнути автоприсудження до мереж Wi-Fi <i>Параметри → Wi-Fi</i> <i>здійснити підключення до довіреної мережі → натиснути знак ⓘ поруч із мережею → вимкнути перемикач Автоприсудження</i> додатково для МКП на iOS: активувати функцію “Приватна адреса Wi-Fi” (для мереж, де пристрій не отримує доступ за MAC-адресою) та “Обмеження відстеження за IP-адресою” <i>Параметри → Wi-Fi</i> <i>Приватна мережа → натиснути знак ⓘ поруч із мережею → також нижче за списком увімкнути перемикач Приватна адреса Wi-Fi</i> <i>а також для будь-яких мереж:</i> <i>Натиснути знак ⓘ поруч із мережею → також нижче за списком увімкнути перемикач Обмеження відстеження за IP-адресою</i>	☐	
11.	Налаштувати максимально безпечний порядок підключення Bluetooth (ретельно перевірити перелік доступних пристроїв та відключити невідомі та непотрібні пристрої) <i>Параметри → Bluetooth → встановити перемикач в положення Включено. Після включення необхідно ретельно перевірити перелік доступних пристроїв, що з'являється, та відключити невідомі та непотрібні пристрої: знайти у списку відповідний пристрій та натиснути знак ⓘ, → натиснути Видалити цей пристрій. По закінченню – вимкнути.</i>	☐	
12.	В налаштуванні параметрів МКП вимкнути голосовий помічник (Siri для iPhone) <i>Параметри → Siri і Пошук → у розділі Запити до Siri переведіть тумблери Чекаати на “Привіт, Siri” та Тиснути бічну кнопку у положення вимкнено, після чого з'явиться запрошення з питанням, чи бажаєте ви повністю відключити Siri. Натисніть підтвердження “Вимкнути Siri”. Потім також деактивуйте всі перемикачі у розділах Зміст від Apple та Пропозиції від Apple. Далі відкрийте пункт Історія Siri й Диктування та натисніть Видалити історію Siri й Диктування</i>	☐	
13.	В налаштуванні параметрів МКП налаштувати блокування екрану МКП через 1 хвилину бездіяльності <i>Параметри → Дисплей і яскравість → Автозамикання → Вибрати відповідний час бездіяльності до блокування</i>	☐	
14.	В налаштуванні параметрів МКП вимкнути можливість попереднього перегляду сповіщень на екрані МКП <i>Параметри → Сповіщення</i> <i>Звіт за розкладом → вимкнути перемикач Звіт за розкладом</i> <i>Передогляд → обрати Ніколи</i> <i>Поширення екрана → вимкнути перемикач Дозволити сповіщення</i> <i>Пропозиції Siri → вимкнути перемикач Дозволити сповіщення</i>	☐	
15.	Перевірити МКП на наявність встановлення підозрілих додатків та додатків соціальних мереж та месенджерів, роботу яких пов'язують із російською федерацією (Viber, Telegram, VK.com, Однокласники, Mail.ru, Яндекс Карти, Яндекс Перекладач, Яндекс Браузер, Яндекс Пошта, Яндекс Перекладач, Яндекс Диск, IVI, MapsMe, 2gis, Getcontact, ДМБ таймер, FaceApp, NewProfilePic, Dr. Web, LinguaLeo, Kaspersky Secure Connection і т.п.), в разі виявлення – видалити (за згодою власника МКП). Опитати власника МКП на рахунок доцільності використання ним додатків, що мало використовуються (мають обмежений, безкорисний функціонал) та видалити такі додатки за згодою власника МКП	☐	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	<i>Довгим натисканням на вибраному/знайденому додатку в Бібліотеці програм в спливаючому вікні вибрати "Вилучити програму" → Вилучити програму</i>		
16.	Перевірити на наявність у календарі пристрою запрошень, свят та інших заходів які власником пристрою не були додані чи заплановані. За згодою власника видалити такі заходи та попередити про недопущення згоди на використання календарю сторонніми програмами (додатками). <i>Календар → На обраній даті перевірити на наявність в переліку заходів не запланованими користувачем та видалити за його згодою</i>	☐	
17.	Оновити встановлені на МКП додатки до останньої доступної версії та активувати функцію їх автооновлення <i>App Store → Обліковий запис → Оновити всі</i>	☐	
18.	Здійснити очищення пам'яті МКП та кешу встановлених додатків на МКП <i>Досягається за рахунок перевстановлення додатку</i>	☐	
19.	Налаштувати максимальне обмеження доступу до конфіденційної інформації (геолокації, стільникових даних, фото галереї, веб-камери, контактів, мікрофону та інше) для кожного встановленого на МКП додатку в залежності від потреби його власника Автоматичне присвоєння геоміток <i>Параметри → Приватність і безпека → Служби локації → у списку програм натиснути Камера → обрати Ніколи</i> Відключення геолокації <i>Параметри → Приватність і безпека → Служби локації: встановити перемикач Служби локації в положення вимкнено; Сигнали геопозиції → встановити перемикач Карта в сигналах геопозиції в положення вимкнено; Моя геопозиція → встановити перемикач Поширювати геопозицію в положення вимкнено; Де iPhone → встановити перемикач Де iPhone в положення вимкнено</i> Відключення відстеження додатками дій користувачів <i>Приватність і безпека → Відстеження → Дозволити програмам надсилати запит на відстеження → встановити перемикач в положення вимкнено</i> Налаштування обмеження доступу <i>Запит на дозвіл має відповідати мінімально необхідному функціоналу програми, а також враховувати міркування безпеки. Наприклад: застосунок з географічними даними може мати доступ до даних геолокації, а якщо програма просить доступ до контактів, галереї, право вносити зміни до пристрою тощо, це вже має бути заборонено. Параметри → Приватність і безпека → налаштувати доступ до кожної категорії інформації (Контакти, Календарі тощо), для чого натискати назву категорії та вимикати всі перемикачі для програм, яким, на Вашу думку, недоцільно надавати доступ до цих категорій інформації</i> Видаляти інформацію про час та місце зйомки <i>Попередити власника МКП, що після відключення присвоєння геоміток, необхідно видалити інформацію про час та місце зйомки на існуючих фото: обрати потрібний файл або декілька файлів у Фотогалереї та: натиснути значок  → у вікні, що відкрилося, змінити → немає місця;</i> Вимкнення персоналізації реклами <i>Параметри → Приватність і безпека → Реклама від Apple → Персоналізована реклама → встановити перемикач в положення вимкнено</i> Відключення сповіщення про ризик зараження Covid-19 <i>Параметри → Сповіщення про контакт → перевірити, що Сповіщення про контактування та Оповістки про наявність вимкнено</i>	☐	
20.	В налаштуванні параметрів МКП вимкнути збір та передачу інформації про мобільний пристрій та збої у його роботі <i>Параметри → Приватність і безпека → Аналітика і Вдосконалення вимкнути Поширювати аналітику iPhone</i>	☐	
21.	В разі необхідності використання власником месенджера Signal, в налаштуваннях Signal необхідно: активувати функцію додаткового захисту доступу до месенджера шляхом введення PIN-коду або використання біометричної автентифікації (сканування обличчя або відбитків пальця)	☐	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	натиснути в лівому верхньому куті екрану піктограму облікового запису → вибрати пункт Налаштування → Обліковий запис → Створіть PIN-код заблокувати можливість реєстрації номеру телефону в месенджері без введення PIN-коду натиснути в лівому верхньому куті екрану піктограму облікового запису → вибрати пункт Налаштування → Обліковий запис → встановити перемикач Блокування реєстрації в положення увімкнено обмежити час зберігання даних в чатах (листування, фото/відео, тощо) мінімальним терміном (за погодженням з власником) натиснути в лівому верхньому куті екрану піктограму облікового запису → вибрати пункт Налаштування → Конфіденційність (Приватність) → Зникаючі повідомлення → обрати мінімальний зручний час, рекомендовано – не більше 1 тижня; зайти по черзі в існуючі чати → натиснути в лівому верхньому куті екрану піктограму чату (групи або контакту) → вибрати пункт Зникаючі повідомлення → мінімальний зручний час, рекомендовано – не більше 1 тижня увімкнути заборону видимості у мережі натиснути в лівому верхньому куті екрану піктограму облікового запису → вибрати пункт Налаштування → Конфіденційність → Додаткові функції → встановити перемикач Завжди ретранслювати дзвінки в положення увімкнено; перемикачі Показувати іконку стану та Дозволити від усіх в положення вимкнено обмежити дозволи для членів груп, які адмініструє власник МКП зайти по черзі в групи, які ви адмініструєте → натиснути в лівому верхньому куті екрану піктограму групи, далі: вибрати пункт Посилання групи → увімкнути групове посилання → встановити перемикач Затвердити нових учасників в положення увімкнено; вибрати пункт Дозволи → у пунктах Додати учасників та Редагувати інформацію про групу обрати пункти Тільки адміністратори видалити невідомі або які не використовуються прив'язані пристрої Налаштування → Прив'язані пристрої → Вибрати пристрій та від'єднати його		
22.	В разі встановлення на МКП інших месенджерів, які у своїх налаштуваннях, окрім згаданого в пункті 11, дозволяють заборонити відображення мобільного номера користувача, вимкнути геолокацію, збір аналітики (у тому числі засобами віртуальної клавіатури), персоналізацію контенту, та налаштування інших параметрів безпеки – все заборонити (відключити), увімкнути двоетапну перевірку (двофакторну автентифікацію), а також перевірити та видалити прив'язані пристрої в налаштуваннях аккаунтів, які невідомі або відомі власнику МКП, проте не використовуються Google Обліковий запис → Налаштування → Дані й конфіденційність → Історія місцезнаходження → Призупинено Обліковий запис → Налаштування → Дані й конфіденційність → Інформація, якою ви можете ділитися з іншими → → Профіль → Ім'я → Будь-хто → Зображення → Лише ви → Стат'я → Лише ви → Дата народження → Лише ви → Електронна адреса → Будь-хто Обліковий запис → Налаштування → Дані й конфіденційність → Інформація, якою ви можете ділитися з іншими → Надсилання геоданих → Ви нікому не надсилаєте свої геодані Обліковий запис → Безпека → → Двоетапна перевірка → Увімкнути → Номер телефону для відновлення → Ввести номер → Резервна електронна адреса → Ввести адресу → Керувати всіма пристроями → Завершити прив'язані пристрої, які не відомі користувачу → Керувати доступом сторонніх додатків → Обрати додаток → Скасувати доступ → Менеджер паролів → Видалити непотрібні паролі	□	

№ з/п	Заходи, які виконуються	Позначка про виконання	Примітка
Перевірка пристрою			
	WhatsApp <i>Налаштування → Підключені пристрої → Завершити прив'язані пристрої, які не відомі користувачу</i> <i>Налаштування → Обліковий запис → Двоетапна перевірка → Увімкнути</i> <i>Налаштування → Конфіденційність →</i> <i>→ Востаннє в мережі й У мережі → Ніхто</i> <i>→ Фото профілю → Ніхто</i> <i>→ Звістка → Ніхто</i> <i>→ Групи → Усі</i> <i>→ Статус → Мої контакти</i> <i>→ Геодані → Немає</i> <i>Налаштування → Конфіденційність → Блокування екрана → Затитувати Face ID</i> <i>→ Увімкнути → Одразу через 1 хвилину</i> Threema <i>Натиснути в правому нижньому куті екрану Налаштування → Блокування за допомогою пароля → Увімкнути введення пароля;</i> <i>натиснути в правому нижньому куті екрану Налаштування → Застосунок/Вебверсія → Прив'язаний пристрій → у переліку пристроїв, що висвітілися, обрати пристрій, який потрібно від'єднати, натиснути на його назву → у діалоговому вікні обрати варіант Ок;</i> <i>натиснути в правому нижньому куті екрану Налаштування → Сповіщення → у секціях У застосунку та Push-сповіщення вимкнути перемикач Попередній перегляд повідомлення;</i> <i>натиснути в правому нижньому куті екрану Налаштування → Блокування за допомогою пароля → Вимагати пароль та обрати мінімальний зручний час (рекомендовано 1 хвилина);</i> <i>натиснути в правому нижньому куті екрану Налаштування → Виклики Threema → встановити перемикач Завжди ретранслювати виклики в положення увімкнено;</i> <i>зайти по черзі в діалоги → натиснути на піктограму контакту → вибрати пункт Рівень підтвердження → разом з кореспондентом виконайте дії, описані у вікні, що з'явиться.</i>		
23.	Змінити мову меню пристрою на раніше обрану (якщо мова змінювалася для проведення налаштувань)	☐	
24.	Забезпечити зміну паролю доступу до МКП його власником <i>Параметри → Face ID і код доступу → Змінити код допуску → вказати новий код</i> <i>→ підтвердити введений код</i>	☐	
25.	Здійснити перезавантаження МКП <i>Одноразове затискання протягом деякого часу клавіш збільшення/зменшення гучності та блокування телефону</i>	☐	
26.	Встановити останнє доступне оновлення для операційної системи, встановленої на МКП та активувати функцію автооновлення <i>Параметри → Загальне → Оновлення ПЗ → в разі наявності доступного оновлення провести його інсталяцію та встановлення → Після оновлення і перезавантаження пристрою → Параметри → Загальне → Оновлення ПЗ → Автооновлення → активувати функцію Викачувати оновлення iOS → активувати функцію Інсталювати оновлення iOS → активувати функцію Безпечні оновлення й системні файли</i>	☐	
27.	Нагадати власнику МКП про необхідність відключати безпроводні мережі (Wi-Fi, Bluetooth, NFC, AirDrop), коли їх робота не потрібна, та перезавантажувати МКП щонайрідше раз на тиждень, краще – щоденно. У разі встановлення нових додатків – контролювати та обмежувати їх дозволи	☐	

(посада, військове звання, підпис, ім'я та прізвище особи, що здійснювала перевірку)

Додаток 4

До Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами (пункт 1.5)

ЗНАК
з попереджувальним написом
(Варіант)



Місце зберігання мобільних електронних пристроїв,
інших електронних засобів - _____

(вказується місце зберігання)

Примітка. Напис на знаку робиться прямим шрифтом на білому фоні. Знак виділяється червоним кольором, інші слова та малюнок виділяються чорним кольором. Розмір знаку з попереджувальним написом – 210х297мм (А4)

Начальник Центрального управління охорони державної таємниці
та захисту інформації Генерального штабу Збройних Сил України
полковник

A handwritten signature in black ink, appearing to read 'Serhiy Dudko'.

Сергій ДУДКО

Додаток 5
До Інструкції зі зберігання і користування
особовим складом Збройних Сил України
мобільними комунікаційними пристроями та
іншими електронними засобами (пункт 4.5)

Перелік
особистих спеціально налаштованих МКП та ІЕЗ
в (назва структурного підрозділу ПУ)

В/звання, ім'я, прізвище відповідального за ЕОМ (електронний засіб)	Найменування та модель ЕОМ (електронного засобу)	Серійний номер ЕОМ (електронного засобу)	MAC-адреса ЕОМ (електронного засобу)	Підрозділ, місце розташування (підключення)	В/звання, ім'я, прізвище осіб, що мають доступ до ЕОМ (електронного засобу)
майор Вячеслав Чернейко	Смартфон Apple iPhone 13 Pro	123456WD89RZ55	6a-78-31-b4-fc-15	Центр зв'язку (місце включення)	майор Вячеслав Чернейко

Начальник служби захисту інформації в автоматизованих системах
(назва структурного підрозділу ПУ)
в/звання

o/n

Ім'я Прізвище