ЗАТВЕРДЖЕНО
Наказ Міністерства оборони України
№

Інструкція
з авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем Міністерства оборони України, Збройних Сил України та Державної спеціальної служби транспорту

Загальні положення

1. Ця Інструкція визначає механізм авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем (далі – ІКС), розпорядниками яких є структурні підрозділи Міністерства оборони України (далі – Міноборони), органи військового управління (крім розвідувального органу Міноборони), військові частини, установи, організації Збройних Сил України (далі – Збройні Сили) та Державної спеціальної служби транспорту (далі – Держспецтрансслужба).

Механізм авторизації локалізованих одномашинних однокористувачевих комплексів Міноборони та Збройних Сил (далі – автоматизовані системи класу “1”) визначається Генеральним штабом Збройних Сил (далі – Генеральний штаб).

2. Авторизація з безпеки ІКС проводиться з метою прийняття рішення щодо можливості функціонування (експлуатації) ІКС з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту.

3. Суб’єктами авторизації з безпеки ІКС є:
галузевий уповноважений орган;
організатор авторизації Міноборони;
організатор авторизації Збройних Сил;
розпорядник ІКС;
підрозділ з оцінювання Міноборони;
підрозділ з оцінювання Збройних Сил;
оцінювач.

4. Реалізація повноважень Міноборони як галузевого уповноваженого органу здійснюється самостійним структурним підрозділом апарату Міноборони, на який, згідно з наказом Міноборони щодо розподілу основних завдань і функцій, визначених Положенням про Міноборони, покладаються функції з розроблення та затвердження галузевих профілів безпеки, а також затвердження цільових профілів безпеки (далі – Галузевий уповноважений орган).

5. Організатором авторизації Міноборони є безпосередньо підпорядкований Міноборони орган військового управління, на який згідно з розподілом повноважень покладено функції з забезпечення технічного захисту інформації в Міноборони (далі – Організатор авторизації Міноборони).

6. Організатором авторизації Збройних Сил є уповноважений орган у сфері технічного захисту інформації Збройних Сил (далі – Організатор авторизації Збройних Сил).

7. Розпорядниками ІКС є самостійні структурні підрозділи апарату Міноборони, безпосередньо підпорядковані Міноборони органи військового управління, установи, організації, військові частини, а також підприємства (їх об’єднання), що належать до сфери управління Міноборони, структурні підрозділи Держспецтрансслужби, структурні підрозділи Апарату Головнокомандувача Збройних Сил, Генерального штабу, органи військового управління, військові частини, вищі військові навчальні заклади, військові навчальні заклади, військові навчальні підрозділи вищих навчальних закладів Збройних Сил, які отримують від власника ІКС право нею розпоряджатися (далі – Розпорядник ІКС).

8. Підрозділами з оцінювання Міноборони є структурні підрозділи Міноборони, органи військового управління, установи, організації (у тому числі військові частини) безпосереднього підпорядкування Міноборони, на які покладено функції (обов’язки) щодо проведення робіт з оцінювання (далі – Підрозділ з оцінювання Міноборони).

9. Підрозділами з оцінювання Збройних Сил є підрозділи технічного захисту інформації, підпорядковані самостійним структурним підрозділам, на які покладено обов’язки щодо виконання завдань з охорони державної таємниці та захисту інформації органів військового управління Збройних Сил (далі – Підрозділ з оцінювання Збройних Сил).

10. Оцінювачами є посадові особи Міноборони, Збройних Сил або Держспецтрансслужби, які є виконавцями робіт з оцінювання дотримання вимог цільових профілів безпеки ІКС (далі – оцінювання), які відповідають встановленим Адміністрацією Держспецзв’язку вимогам (далі – Оцінювач).

11. Об’єктом авторизації з безпеки є ІКС, яка підлягає оцінюванню відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту.

Авторизація з безпеки ІКС здійснюється з метою прийняття рішення щодо можливості функціонування (експлуатації) ІКС.

12. Галузевий уповноважений орган здійснює такі основні функції:

1) розробляє та підтримує в актуальному стані галузеві профілі безпеки (далі – ГПБ) для ІКС Міноборони, Збройних Сил та Держспецтрансслужби;

2) розробляє рекомендації, організаційно-розпорядчі документи щодо розробки та впровадження цільових профілів безпеки (далі – ЦПБ) ІКС, проведення оцінки ризиків щодо ІКС, яка підлягає авторизації з безпеки (далі – оцінка ризиків), оцінювання та авторизації з безпеки ІКС;

3) здійснює контроль за станом впровадження заходів захисту інформації, передбачених ЦПБ;

4) затверджує ЦПБ для ІКС Міноборони, Збройних Сил та Держспецтрансслужби, за винятком ЦПБ для автоматизованих систем класу “1”;

5) доводить до Організатора авторизації Міноборони та Організатора авторизації Збройних Сил, а також до Розпорядників ІКС зміни до ГПБ;

6) здійснює взаємодію з Адміністрацією Держспецзв’язку з метою реалізації процедури авторизації з безпеки в Міноборони, Збройних Силах та Держспецтрансслужбі, у тому числі щодо формування та впровадження ГПБ.

13. Організатор авторизації Міноборони здійснює такі основні функції:

1) приймає рішення щодо визначення Оцінювачів або Підрозділу з оцінювання Міноборони для проведення робіт з оцінювання;

2) організовує та забезпечує проведення оцінювання ІКС Міноборони;

3) забезпечує неупереджене, об’єктивне та своєчасне проведення оцінювання;

4) надає Розпоряднику ІКС методичну допомогу щодо розроблення та впровадження ЦПБ, виконання підготовчих заходів для проведення оцінювання;

5) забезпечує підготовку, навчання та підтримання належного рівня компетенцій Оцінювачів;

6) щорічно перевіряє рівень компетенції (кваліфікації) Оцінювачів з урахуванням вимог професійного стандарту фахівця з оцінювання заходів захисту інформації, затвердженого Адміністрацією Держспецзв’язку;

7) веде перелік Оцінювачів в межах Міноборони;

8) забезпечує дотримання принципу незалежності Оцінювачів шляхом недопущення залучення до оцінювання фахівців, які брали участь у розробці та/або впровадженні заходів захисту інформації, визначених ЦПБ.

14. Організатор авторизації Збройних Сил здійснює такі основні функції:

1) приймає рішення щодо визначення Оцінювачів або Підрозділу з оцінювання Збройних Сил для проведення робіт з оцінювання;

2) може делегувати повноваження щодо визначення Оцінювачів (із відомчого переліку оцінювачів) або Підрозділу з оцінювання Збройних Сил для проведення робіт з оцінювання ІКС Збройних Сил управлінням (відділам) охорони державної таємниці та захисту інформації органів військового управління Збройних Сил;

3) організовує та забезпечує проведення оцінювання ІКС Збройних Сил;

4) забезпечує неупереджене, об'єктивне та своєчасне проведення оцінювання;

5) надає Розпоряднику ІКС методичну допомогу щодо розроблення та впровадження ЦПБ, виконання підготовчих заходів для проведення оцінювання;

6) веде перелік Оцінювачів у межах Збройних Сил;

7) забезпечує підготовку, навчання та підтримання належного рівня компетенцій Оцінювачів;

8) щорічно перевіряє рівень компетенції (кваліфікації) Оцінювачів з урахуванням вимог професійного стандарту фахівця з оцінювання заходів захисту інформації, затвердженого Адміністрацією Держспецзв'язку;

9) може визначати структурний підрозділ для надання Розпоряднику ІКС методичної допомоги щодо порядку та організації проведення авторизації з безпеки ІКС;

10) забезпечує дотримання принципу незалежності Оцінювачів шляхом недопущення залучення до оцінювання фахівців, які брали участь у розробці та/або впровадженні заходів захисту інформації, визначених ЦПБ.

15. Адміністрація Держспецтранслужби щодо авторизації з безпеки ІКС здійснює такі основні функції:

1) погоджує ЦПБ для ІКС, розпорядником яких є Держспецтранслужба;

2) веде перелік Оцінювачів у межах Держспецтранслужби (за їх наявності);

3) здійснює взаємодію з Організатором авторизації Збройних Сил або Організатором авторизації Міноборони щодо організації оцінювання, а також щодо формування та впровадження вимог ЦПБ.

16. Розпорядник ІКС здійснює такі основні функції:

1) проводить щорічну оцінку ризиків, а також оцінку ризиків при внесенні змін в архітектуру ІКС, що впливають на її безпеку;

2) організовує проведення експертної оцінки інформації, яка обробляється або планується до обробки в ІКС;

3) розробляє ЦПБ за формою, визначеною додатком 1, з урахуванням ГПБ або базового профілю безпеки (далі – БПБ) – у разі відсутності ГПБ;

4) організовує впровадження вимог ЦПБ;

5) переглядає ЦПБ не рідше одного разу на рік, вносить зміни до нього у разі змін до БПБ та/або ГПБ, а також за результатами проведеної оцінки ризиків щодо ІКС;

6) проводить попереднє оцінювання дотримання вимог ЦПБ, затверджує Акт за результатами попереднього оцінювання впровадження вимог ЦПБ;

7) надає Організатору авторизації та Оцінювачам достовірні відомості про ІКС, щодо якої здійснюється оцінювання, а також доступ до ІКС, приміщень, необхідної документації тощо для проведення відповідних робіт з оцінювання;

8) погоджує План проведення оцінювання (додаток 2);

9) оформлює проєкт авторизаційного листа за формою, визначеною додатком 1 до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 року № 712, та направляє його до Галузевого уповноваженого органу;

10) щодо ІКС, в якій обробляється інформація, що становить державну таємницю, надсилає до Галузевого уповноваженого органу авторизаційну документацію, яка визначена пунктом 69 цієї Інструкції, разом із проєктом авторизаційного листа;

11) здійснює контроль за реалізацією заходів захисту інформації, визначених ЦПБ, та дотриманням визначених термінів їх проведення.

17. Підрозділ з оцінювання Міноборони здійснює такі основні функції:

1) визначає Оцінювачів для проведення оцінювання;

2) затверджує План проведення оцінювання, а у випадку делегування Організатором авторизації Міноборони повноважень щодо визначення Оцінювачів – затверджує Звіт за результатами проведення оцінювання (додаток 3);

3) може надавати методичні рекомендації Розпоряднику ІКС щодо проведення авторизації з безпеки;

9) підтримує та перевіряє рівень компетенції (кваліфікації) Оцінювачів з урахуванням вимог професійного стандарту фахівця з оцінювання заходів захисту інформації, затвердженого Адміністрацією Держспецзв'язку;

4) інформує Організатора авторизації Міноборони та Розпорядника ІКС про виявлені недоліки або проблемні питання, виявлені в процесі оцінювання ІКС.

18. Підрозділ з оцінювання Збройних Сил здійснює такі основні функції:

1) визначає Оцінювачів для проведення оцінювання;

2) затверджує План проведення оцінювання та Звіт за результатами проведення оцінювання – у випадку делегування Організатором авторизації Збройних Сил повноважень щодо визначення Оцінювачів;

3) може надавати Розпоряднику ІКС методичні рекомендації щодо проведення авторизації з безпеки;

4) підтримує та перевіряє рівень компетенції (кваліфікації) Оцінювачів з урахуванням вимог професійного стандарту фахівця з оцінювання заходів захисту інформації, затвердженого Адміністрацією Держспецзв'язку;

5) інформує Організатора авторизації Збройних Сил та Розпорядника ІКС про недоліки або проблемні питання, виявлені в процесі оцінювання ІКС.

19. Оцінювач здійснює такі основні функції:

1) за дорученням Організатора авторизації Міноборони, Організатора авторизації Збройних Сил, керівника Підрозділу з оцінювання Міноборони або керівника Підрозділу з оцінювання Збройних Сил проводить оцінювання ІКС Міноборони або Збройних Сил, або Держспецтрансслужби;

2) розробляє План проведення оцінювання, інші необхідні документи для проведення оцінювання, а також оформлює Звіт за результатами проведення оцінювання;

3) повідомляє Розпорядника ІКС та відповідного Організатора авторизації про виявлені недоліки, а також надає рекомендації щодо їх усунення;

4) надає рекомендації щодо удосконалення реалізації заходів захисту інформації, передбачених ЦПБ;

5) отримує від Розпорядника ІКС усі відомості, матеріали тощо, необхідні для проведення оцінювання;

6) зобов'язується неухильно дотримуватися вимог законодавства, національних стандартів, нормативних документів у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту, а також відповідних наказів та рішень органів військового управління.

20. Під час проведення оцінювання Оцінювач повинен дотримуватися таких принципів:

1) доброчесності (діяти відповідально, чесно та неупереджено, демонструючи високі етичні стандарти);

2) об'єктивності (забезпечувати правдиве та точне відображення результатів оцінювання, базуючись виключно на фактах);

3) професійного підходу (приймати обґрунтовані рішення на основі знань, досвіду та вимог законодавства, національних стандартів та нормативних документів у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту);

4) конфіденційності (забезпечувати захист та нерозголошення інформації, отриманої під час проведення оцінювання, у тому числі після його завершення, за винятком випадків, передбачених законодавством України та цією Інструкцією);

5) незалежності (уникати конфлікту інтересів, зокрема не здійснювати оцінювання ІКС, у розробленні чи впровадженні яких оцінювач брав участь);

6) доказового підходу (формувати висновки та рекомендації виключно на основі достатніх, належних та переконливих доказів).

21. Авторизація з безпеки системи здійснюється для ІКС, щодо яких затверджено ЦПБ.

22. Авторизація з безпеки ІКС може бути первинною, плановою, позаплановою.

23. Первинна авторизація з безпеки ІКС є основним видом авторизації та здійснюється з метою прийняття рішення щодо можливості функціонування (експлуатації) ІКС.

24. Планова авторизація з безпеки ІКС проводиться з метою підтвердження авторизації за результатами перегляду ЦПБ на підставі щорічної оцінки (перегляду) ризиків. Вона здійснюється протягом життєвого циклу ІКС, не пізніше одного календарного року після проведення первинної, планової або позапланової авторизації з безпеки ІКС.

У разі відсутності зміни умов функціонування (експлуатації) ІКС, які призводять до появи нових ризиків та/або модернізації ІКС, що впливає на реалізацію вимог з безпеки зі складу ЦПБ (зокрема зміни ІКС, її архітектури та/або складу тощо) оцінювання може не проводитись. У такому випадку авторизаційний лист формується на основі проведеної оцінки ризиків із посиланням на попередній Звіт за результатами проведення оцінювання.

25. Позапланова авторизація з безпеки ІКС проводиться у разі:

1) внесення змін до БПБ або ГПБ, на підставі якого був сформований ЦПБ, якщо інше не передбачено актами, якими затверджено БПБ або ГПБ;

2) внесення змін до ЦПБ, у тому числі в результаті зміни умов функціонування (експлуатації) ІКС, які призведуть до появи нових ризиків та/або модернізації ІКС, що впливає на реалізацію заходів захисту інформації зі складу ЦПБ (зміни ІКС, її архітектури та/або складу тощо);

3) внесення змін до ЦПБ за результатами державного контролю за додержанням вимог законодавства у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту, стану технічного або криптографічного захисту.

26. Позапланова авторизація з безпеки ІКС проводиться протягом шести місяців з дати внесення змін до БПБ, ГПБ або ЦПБ, якщо інше не передбачено нормативно-правовими актами.

27. Оцінювання в рамках позапланової авторизації з безпеки може проводитись в частині внесених змін до ІКС або ЦПБ або в повному обсязі – за рішенням Розпорядника ІКС.

28. Авторизація з безпеки ІКС здійснюється в такій послідовності:

1) розроблення та затвердження ЦПБ;

2) виконання вимог ЦПБ;

3) оцінювання дотримання вимог ЦПБ;

4) створення комплексу технічного захисту інформації (далі – КТЗІ) для захисту інформації від витоку технічними каналами (у випадку обробки в ІКС інформації, що становить державну таємницю);

5) оцінка відповідності КТЗІ (у випадку обробки в ІКС інформації, що становить державну таємницю);

6) оформлення та подання до Адміністрації Держспецзв’язку авторизаційного листа для внесення даних щодо авторизації з безпеки ІКС до переліку авторизованих систем з безпеки.

29. Роботи щодо розробки та виконання вимог ЦПБ, а також щодо впровадження КТЗІ можуть проводитись паралельно.

Розроблення та затвердження ЦПБ

30. Розроблення та затвердження ЦПБ здійснюється з урахуванням вимог законодавства, національних стандартів та нормативних документів у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту, відповідних наказів, рішень органів військового управління, а також рекомендацій, визначених Галузевим уповноваженим органом.

31. До початку розроблення ЦПБ Розпорядник ІКС зобов’язаний провести інвентаризацію активів ІКС та оцінку ризиків.

32. За результатами інвентаризації активів ІКС формується реєстр, який повинен містити:

1) інформаційні активи (дані, бази даних, файли тощо);

2) апаратні активи (серверне та мережеве обладнання, робочі станції, мобільні пристрої тощо);

3) програмні активи (системні і прикладні комп’ютерні програми (застосунки);

4) фізичні активи (приміщення, охоронно-пожежна сигналізація, системи контролю доступу, системи електроживлення тощо);

5) персонал (користувачі, адміністратори, служба підтримки, постачальники тощо);

6) документація (політики, описи, порядки, інструкції тощо).

33. Для інформаційних активів зазначається ступінь обмеження доступу інформації, яка обробляється в ІКС, форма відображення або зберігання інформації, місце зберігання та інша інформація (за необхідності).

34. Для активу “персонал” зазначаються ролі та повноваження відповідних суб’єктів в ІКС, включаючи їх ролі в прикладному програмному забезпеченні.

35. При проведенні оцінки ризиків рекомендовано використовувати методології, визначені в ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки ” або NIST Special Publication 800-30 “Guide for Conducting Risk Assessments”.

Розпорядник ІКС може використовувати інші методології за умови забезпечення належного рівня управління ризиками.

36. Під час проведення оцінки ризиків Розпорядник ІКС може залучати розробника ІКС, відповідального за реагування на кіберінциденти, відповідального за проєктування ІКС, відповідального за функціонування ІКС, а також інших суб'єктів − за потреби.

37. За результатами проведеної оцінки ризиків Розпорядник ІКС оформлює та затверджує в установленому порядку звіт за результатом проведення оцінки ризиків. Окрім іншого, такий звіт має містити обґрунтування щодо вибору заходів захисту інформації, які будуть включені до ЦПБ.

38. ЦПБ розробляється для кожної ІКС, яка підлягає авторизації. Він повинен враховувати вимоги БПБ та ГПБ, вимоги законодавства, національних стандартів та нормативних документів у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту, відомчі вимоги, політики безпеки, призначення ІКС, її структурно-функціональні характеристики та особливості функціонування, результати проведеної оцінки (аналізу) ризиків.

39. ЦПБ розробляється Розпорядником ІКС, погоджується з Організатором авторизації, затверджується Розпорядником ІКС та Галузевим уповноваженим органом.

ЦПБ для ІКС, розпорядником якої є підрозділ Збройних Сил, погоджується з Організатором авторизації Збройних Сил.

ЦПБ для ІКС, розпорядником якої є структурний підрозділ Міноборони, погоджується з Організатором авторизації Міноборони.

ЦПБ для ІКС, розпорядником якої є структурний підрозділ Держспецтрансслужби, погоджується Адміністрацією Держспецтрансслужби та затверджується Галузевим уповноваженим органом.

40. Для погодження ЦПБ Розпорядник ІКС надсилає на адресу Організатора авторизації ЦПБ звіт за результатами оцінки ризиків, технічне завдання на створення (модернізацію) ІКС, опис ІКС (за наявності).

41. Розгляд ЦПБ здійснюється Організатором авторизації протягом десяти робочих днів з дати його надходження.

За результатами розгляду ЦПБ Організатор авторизації погоджує або надає зауваження до нього.

42. Погоджений ЦПБ, а також документи, визначені пунктом 41 цієї Інструкції, повертаються Організатором з авторизації Розпоряднику ІКС.

43. Для затвердження ЦПБ Розпорядник ІКС надсилає на адресу Галузевого уповноваженого органу ЦПБ та звіт за результатами оцінки ризиків у двох примірниках.

За результатом затвердження ЦПБ перший примірник вказаних документів повертається Розпоряднику ІКС, а другий примірник залишається в Галузевому уповноваженому органі.

Виконання вимог ЦПБ

44. Виконання (впровадження) вимог ЦПБ, зокрема проведення робіт із захисту інформації та кібербзахисту в ІКС, здійснюється підрозділом із кіберзахисту (службою захисту інформації в автоматизованих системах) Розпорядника ІКС або призначеними особами, які здійснюють впровадження заходів із захисту інформації в ІКС.

Під час виконання вимог ЦПБ Розпорядником ІКС можуть залучатися розробник ІКС, відповідальний за реагування на кіберінциденти, відповідальний за проєктування ІКС, відповідальний за функціонування ІКС, а також інші суб'єкти – за потреби.

45. З метою реалізації вимог ЦПБ Розпорядник ІКС затверджує план захисту інформації та кібербезпеки, в якому, зокрема, зазначаються заходи захисту інформації, їх детальний опис, способи та засоби їх реалізації, відповідальні за впровадження кожного з заходів, а також терміни їх впровадження. Для розроблення вказаного плану пропонується враховувати рекомендації Національного інституту стандартів і технологій Сполучених Штатів Америки NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems.

46. За результатами виконання вимог ЦПБ Розпорядником ІКС затверджуються:

1) рішення щодо проведення авторизації з безпеки ІКС (наказ Розпорядника ІКС);

2) перелік інформації, що підлягає обробленню та захисту в ІКС;

3) акт категоріювання об'єкта інформаційної діяльності (для ІКС, в яких здійснюється обробка відкритої, конфіденційної або службової інформації – категоріювання не здійснюється);

4) звіт за результатами оцінки ризиків;

5) ЦПБ;

6) план захисту інформації та кібербезпеки;

7) політики безпеки (порядки, правила тощо), визначені ЦПБ або нормативними документами у сферах технічного захисту інформації, криптографічного захисту інформації, а також кіберзахисту;

8) експлуатаційна документація (інструкції, настанови тощо);

9) рішення на створення КТЗІ (у разі обробки в ІКС інформації, що становить державну таємницю, та наявності окремого рішення).

47. Результатом виконання вимог ЦПБ для ІКС, в яких обробляється, (планується оброблятися) інформація, що становить державну таємницю, є затверджена Розпорядником ІКС документація, визначена пунктом 46 цієї Інструкції, та документ про оцінку відповідності КТЗІ, який затверджується керівником підрозділу, який здійснював оцінку відповідності КТЗІ.

48. Документацію, необхідну для проведення авторизації з безпеки, дозволяється вести в електронному вигляді відповідно до вимог законодавства.

49. Описи ІКС, експлуатаційну документацію дозволяється вести в електронному вигляді.

50. За результатами виконання вимог ЦПБ Розпорядник ІКС проводить попереднє оцінювання впровадження вимог ЦПБ та у встановленому порядку затверджує акт за результатами виконання таких робіт.

Впровадження та атестація КТЗІ

51. Порядок проведення робіт зі створення та атестації КТЗІ визначається Генеральним штабом з урахуванням вимог, визначених Адміністрацією Держспецзв’язку.

52. Розпорядники ІКС, у яких обробляється державна таємниця, керуються вимогами Генерального штабу щодо порядку проведення робіт зі створення та атестації КТЗІ.

Проведення оцінювання дотримання вимог ЦПБ

53. Підставою для проведення оцінювання є завершення Розпорядником ІКС впровадження вимог ЦПБ, що підтверджується позитивним висновком за результатами попереднього оцінювання, проведеного Розпорядником ІКС.

54. З метою залучення Оцінювачів для проведення оцінювання Розпорядник ІКС подає Організатору авторизації заявку в довільній формі, у якій зазначаються відомості про результати попереднього оцінювання, впровадження вимог ЦПБ, а також реквізити акта за результатами проведення таких робіт.

Заявка на проведення оцінювання ІКС Збройних Сил або ІКС Держспецтрансслужби надсилається до Організатора авторизації Збройних Сил.

Заявка на проведення оцінювання ІКС Міноборони надсилається до Організатора авторизації Міноборони.

55. Залучення Оцінювачів Міноборони до оцінювання ІКС Збройних Сил здійснюється за погодженням з Організатором авторизації Збройних Сил.

Залучення Оцінювачів Збройних Сил до оцінювання ІКС Міноборони здійснюється за погодженням з Організатором авторизації Міноборони.

Формування спільних груп Оцінювачів для проведення оцінювання ІКС Міноборони, Збройних Сил та Держспецтрансслужби здійснюється за рішенням заступника Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації (далі – заступник Міністра), за поданням відповідного Організатора авторизації.

56. У разі неможливості залучення Оцінювачів, визначених пунктами 54 та 55 цієї Інструкції, Розпорядник ІКС може прийняти рішення про залучення до проведення оцінювання відповідних суб'єктів оцінювання з урахуванням вимог пункту 3 Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури, затвердженого постановою Кабінету Міністрів України від 31 грудня 2025 року № 1799.

У разі прийняття Розпорядником ІКС рішення про залучення до проведення робіт з оцінювання відповідних суб'єктів оцінювання, зазначених в абзаці першому цього пункту, таке залучення здійснюється на підставі укладеного в установленому порядку договору, який повинен містити вимоги щодо дотримання процедур проведення оцінювання, визначених цією Інструкцією.

57. Оцінювання здійснюється з урахуванням вимог (рекомендацій) Адміністрації Держспецзв'язку та Галузевого уповноваженого органу.

58. Для проведення оцінювання Оцінювачем або залученим за рішенням Розпорядника ІКС суб'єктом оцінювання розробляється План проведення оцінювання, який погоджується Розпорядником ІКС та затверджується Організатором авторизації.

Такий План повинен містити перелік заходів захисту інформації, що мають бути оцінені, методи оцінювання та строки проведення оцінювання.

59. Під час проведення оцінювання Оцінювач може використовувати такі методи оцінювання всіх складових середовищ функціонування ІКС (фізичного, обчислювального, інформаційного або середовища користувачів), що підлягають оцінюванню, з метою підтвердження ефективності впровадження та функціонування заходів захисту інформації (далі – об'єкти оцінювання):

1) метод дослідження – процес огляду, вивчення, інспектування, спостереження або аналізу об'єктів оцінювання;

2) метод опитування – процес проведення інтерв'ю з окремими особами або групами осіб, які мають безпосереднє відношення щодо об'єктів оцінювання;

3) метод випробування – процес дослідження об'єктів оцінювання шляхом ініціювання та перевірки функціонування їхніх технічних і програмних засобів, а також механізмів захисту в заздалегідь визначених або модельованих умовах з

метою порівняння фактичних результатів їхньої роботи з очікуваними результатами та встановленими вимогами.

60. У разі застосування Оцінювачем під час проведення робіт з оцінювання методу опитування, у Звіті за результатами проведення оцінювання зазначаються посадові особи, з якими було проведено інтерв'ю, а також результати такого інтерв'ю.

61. За результатами оцінювання Оцінювачем оформлюється Звіт за результатами проведення таких робіт.

Звіт за результатами проведення оцінювання затверджується Організатором авторизації Збройних Сил або Організатором авторизації Міноборони.

62. Звіт за результатами оцінювання має включати такі відомості:

1) назва ІКС;
2) вищий ступінь обмеження доступу до інформації, що обробляється в ІКС;
3) дата(и) оцінювання;
4) відомості про Оцінювача;
5) позначення вимог з безпеки інформації та зміст заходів із захисту інформації;
6) вибрані методи та об'єкти оцінювання;
7) посилання на розпорядчі документи, яким регулюються вимоги з безпеки;
8) результат оцінювання (із зазначенням "позитивний", якщо всі вимоги з безпеки, передбачені БПБ, ГПБ (за наявності) та ЦПБ, реалізовані або "негативний", якщо одна або декілька вимог з безпеки, передбачені БПБ, ГПБ (за наявності) та ЦПБ, не реалізовані);
9) коментарі Оцінювача (зауваження або недоліки);
10) висновки щодо результату проведеного оцінювання та рекомендації (виправлення, коригувальні дії або покращення);
11) додаткова інформація (за потреби).

63. До Звіту за результатами проведення оцінювання додаються докази щодо реалізації заходів захисту інформації (у вигляді скріншотів, фотографій тощо). Такі докази можуть бути записані у вигляді файлів на окремому матеріальному носії інформації з унеможливленням внесення змін до них або шляхом накладання електронного цифрового підпису на такі файли. Докази щодо проведення оцінювання зберігаються разом зі Звітом за результатами проведення оцінювання.

64. У випадку позитивного результату оцінювання Оцінювачем можуть бути надані рекомендації щодо удосконалення реалізації одного або декількох заходів захисту інформації (вимог з безпеки), про що окремо зазначається у Звіті за результатами проведення оцінювання. Рішення щодо реалізації наданих

рекомендацій приймається Розпорядником ІКС з урахуванням можливих ризиків.

65. У разі прийняття Оцінювачем негативного рішення у Звіті за результатами проведення оцінювання зазначається інформація про виявлені недоліки та заходи, які необхідно вжити для їх усунення.

66. Розпорядником ІКС за результатами усунення виявлених недоліків проводиться повторна процедура оцінювання заходів захисту інформації або вимог з безпеки інформації, щодо яких були виявлено недоліки.

67. У разі якщо усунення недоліків потребує значного часу (більше шести місяців), поводиться повторне оцінювання дотримання вимог ЦПБ.

Оформлення та подання авторизаційного листа

68. На підставі Звіту за результатами проведення оцінювання та наданих Оцінювачем рекомендацій Розпорядник ІКС приймає рішення щодо оформлення проєкту авторизаційного листа та надсилає його разом зі Звітом за результатами проведення оцінювання та доказами до нього до Галузевого уповноваженого органу.

69. У разі авторизації ІКС, в якій обробляється інформація, що становить державну таємницю, окрім документів, визначених пунктом 68 цієї Інструкції, разом з проєктом авторизаційного листа на адресу Галузевого уповноваженого органу надсилається:

1) копія затвердженого ЦПБ для ІКС, щодо якої здійснюється авторизація;
2) примірник Звіту за результатами проведення оцінювання;
3) примірник документа про оцінку відповідності КТЗІ.

70. Галузевий уповноважений орган здійснює аналіз наданої Розпорядником ІКС документації та у разі відсутності зауважень подає проєкт авторизаційного листа на підпис заступнику Міністра. При цьому один примірник Звіту за результатами проведення оцінювання повертається Розпоряднику ІКС, а інший – залишається в Галузевому уповноваженому органі.

У разі виявлення недоліків щодо правильності та повноти обраних засобів і методів, визначених у цільовому профілі, або невідповідності впроваджених заходів захисту інформації вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту, Галузевий уповноважений орган повертає документацію Розпоряднику ІКС на доопрацювання та інформує заступника Міністра про підстави такого повернення.

71. Підписаний заступником Міністра авторизаційний лист направляється Галузевим уповноваженим органом до Адміністрації Держспецзв'язку для включення такої ІКС до переліку авторизованих систем з безпеки.

Для ІКС, у яких обробляється державна таємниця, Галузевий уповноважений орган разом з авторизаційним листом надсилає до Адміністрації Держспецзв'язку документи, визначені підпунктами 1-3 пункту 69 цієї Інструкції.

72. Після надходження від Адміністрації Держспецзв'язку повідомлення про включення ІКС до переліку авторизованих систем з безпеки Галузевий уповноважений орган направляє відповідне повідомлення Організатору авторизації та Розпоряднику ІКС.

73. Після отримання повідомлення про включення ІКС до переліку авторизованих систем з безпеки Розпорядник ІКС повинен направити копію Звіту за результатами проведення оцінювання до Адміністрації Держспецзв'язку.

Скасування авторизації з безпеки ІКС

74. Авторизація з безпеки ІКС може скасовуватися у таких випадках:

1) прийняття Адміністрацією Держспецзв'язку рішення за результатами розгляду письмового звернення Розпорядника ІКС про скасування авторизації з безпеки, про що Розпорядник ІКС повідомляє відповідного Організатора авторизації;

2) непроведення Розпорядником ІКС у встановлені строки планової авторизації з безпеки;

3) непроведення Розпорядником ІКС позапланової авторизації з безпеки протягом шести місяців з дати внесення змін до БПБ, ГПБ або ЦПБ;

4) невиконання Розпорядником ІКС у встановлені строки вимог щодо усунення порушень, виявлених за результатами проведення державного контролю за додержанням вимог законодавства у сферах технічного захисту інформації, криптографічного захисту інформації та кіберзахисту.

75. У разі скасування авторизації з безпеки ІКС проводиться первинна авторизація з урахуванням вимог, визначених цією Інструкцією.

Директор Директорату цифрової трансформації
у сфері оборони Міністерства оборони України
майор Артем РОМАНЮКОВ

Додаток 1
до Інструкції з авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем Міністерства оборони України, Збройних Сил України та Державної спеціальної служби транспорту
(пункт 16)

ГОД
Прим.№ ___

ЗАТВЕРДЖУЮ

_____
(посада керівника установи установи–Розпорядника ІКС)

_____ _____
(підпис) (Ім'я, прізвище)

_____ _____ _____
(дата)

ЗАТВЕРДЖУЮ

_____
(посада керівника установи установи–Галузевого уповноваженого органу)

_____ _____
(підпис) (Ім'я, прізвище)

_____ _____ _____
(дата)

ПОГОДЖЕНО

_____
(посада керівника установи установи–Організатора авторизації)

_____ _____
(підпис) (Ім'я, прізвище)

_____ _____ _____
(дата)

ЦІЛЬОВИЙ ПРОФІЛЬ БЕЗПЕКИ ІНФОРМАЦІЇ
інформаційно-комунікаційної системи

_____
(назва інформаційно-комунікаційної системи)

1. Загальні положення

1.1. Цільовий профіль безпеки інформації інформаційно-комунікаційної системи _____ (далі – Цільовий профіль)
(назва інформаційно-комунікаційної системи)

встановлює набір вимог з безпеки інформації та заходів захисту інформації для інформації інформаційно-комунікаційної системи (далі – ІКС)

_____
(назва інформаційно-комунікаційної системи)

Продовження додатка 1

1.2. Вказуються терміни та визначення, які вживаються в даному документі.

1.3. Підстава розробки Цільового профілю

_____,
(базовий профіль безпеки системи, на основі якого розроблений цільовий профіль безпеки системи, а також реквізити наказу, яким його затверджено)

_____,
(галузевий профіль безпеки системи, на основі якого розроблений цільовий профіль безпеки системи, а також реквізити наказу, яким його затверджено)

_____,
(реквізити проведеної експертної оцінки інформації, яка обробляється (оброблятиметься) в системі, рішення на проведення авторизації з безпеки або рішення на створення системи, а також інші нормативні документи в сфері технічного та криптографічного захисту інформації, кіберзахисту)

1.4. Заходи захисту Цільового профілю визначені відповідно до вимог _____
(стандарт, НД ТЗІ, згідно якого обрано заходи захисту)

2. Вимоги з безпеки інформації ІКС

2.1. _____
(назва блоку вимог обраного базового профілю безпеки системи)

2.1.1. _____
(назва вимоги (дії) з безпеки відповідно до базового профілю безпеки системи)

Номер вимоги базового/галузевого профіля: _____
(номер відповідно до обраного базового/галузевого профілю безпеки системи)

Вимога:

_____
(зміст вимоги (дії) з безпеки, відповідно до обраного базового/галузевого профілю безпеки системи)

Визначені параметри вимоги:

Параметр	Значення параметру

Заходи захисту відповідно до_____:
(стандарт, НД ТЗІ, згідно якого обрано заходи захисту)

_____
(позначення заходів захисту відповідно до обраного стандарту або НД ТЗІ)

2.1.1.1. _____
(назва заходу захисту відповідно до обраного стандарту або НД ТЗІ)

Продовження додатка 1

Номер заходу: _____
(позначення заходу захисту відповідно до обраного стандарту або НД ТЗІ)

Заходи захисту:

_____
(формулювання заходу захисту відповідно до обраного стандарту або НД ТЗІ)

Визначені параметри заходу захисту:

Параметр	Значення параметру

_____
(посада керівника підрозділу з кіберзахисту-розробника ЦПБ)

_____ _____
(підпис) (Ім’я, прізвище)

Додаток 2
до Інструкції з авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем Міністерства оборони України, Збройних Сил України та Державної спеціальної служби транспорту
(пункт 16)

ПОГОДЖЕНО

_____
(посада керівника установи)

_____ _____
(підпис) (Ім’я, прізвище)

_____ _____ _____
(дата)

ЗАТВЕРДЖУЮ

_____
(посада керівника установи –
Організатора/Підрозділу з оцінювання)

_____ _____
(підпис) (Ім’я, прізвище)

_____ _____ _____
(дата)

ПЛАН
проведення оцінювання дотримання вимог цільових профілів безпеки інформаційно-комунікаційної системи

_____
(назва інформаційно-комунікаційної системи)

Продовження додатка 2

І ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Призначення оцінювання дотримання вимог цільових профілів безпеки
1.2 Відомості щодо оцінювачі, які проводять роботи з оцінювання
1.3 Методика проведення оцінки
1.4 Загальні відомості щодо оцінювання

ІІ ОЦІНКА РЕАЛІЗАЦІЇ ЦІЛЬОВОГО ПРОФІЛЮ БЕЗПЕКИ

Номер вимоги	Назва вимоги з безпеки інформації	Захід захисту інформації відповідно до НД ТЗІ 3.6-006-24	Назва заходу захисту інформації	Дата проведення робіт	Відповідальний (зі сторони Розпорядника)

_____
(посада Оцінювача)

_____ _____
(підпис) (Ім’я, прізвище)

Додаток 3
до Інструкції з авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем Міністерства оборони України, Збройних Сил України та Державної спеціальної служби транспорту
(пункт 17)

ЗАТВЕРДЖУЮ

_____
(посада керівника установи – Підрозділу з оцінювання)

_____ _____
(підпис) (Ім’я, прізвище)

_____ _____ _____
(дата)

ЗВІТ
за результатами проведення оцінювання дотримання вимог цільових профілів безпеки інформаційно-комунікаційної системи

_____
(назва інформаційно-комунікаційної системи)

Продовження додатка 3

1. Загальні положення

_____

(мета проведення робіт, методи використані під час оцінювання та іншу інформацію (за необхідності))

2. Відомості про оцінювачів

_____

(відомості про оцінювачів)

3. Вимоги з безпеки інформації інформаційно-комунікаційної систем _____

(назва інформаційно-комунікаційної системи)

3.1._____

(назва блоку вимог обраного базового/галузевого профілю безпеки системи)

3.1.1. _____

(назва вимоги (дії) з безпеки відповідно до базового/галузевого профілю безпеки системи)

Номер вимоги базового профіля: _____

(номер відповідно до обраного базового/галузевого профілю безпеки системи)

Вимога:

_____

(зміст вимоги (дії) з безпеки, відповідно до обраного базового профілю безпеки системи)

Заходи захисту відповідно до_____: _____

(стандарт, НД ТЗІ, згідно якого обрано заходи захисту) (позначення заходів захисту відповідно до обраного стандарту або НД ТЗІ)

3.1.1.1._____.

(назва заходу захисту відповідно до обраного стандарту або НД ТЗІ)

Номер заходу: _____

(позначення заходу захисту відповідно до обраного стандарту або НД ТЗІ)

Продовження додатка 3

Заходи захисту:	Докази, джерела отримання відомостей

Висновок з оцінки – _____.
(реалізовано/не реалізовано)

Рекомендації з покращення (коментарі оцінювачів): _____
(рекомендації з покращення, особливі думки Оцінювача(ів), за наявності)

_____
(посада Оцінювача)

_____ _____
(підпис) (Ім’я, прізвище)

Примітка. Звіт зберігається протягом трьох років.