НОРМАТИВНИЙ ДОКУМЕНТ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Технічний захист інформації на програмно-керованих АТС загального користування Специфікації гарантій захисту

Департамент спеціальних телекомунікаційних систем та захисту інформації
Служби безпеки України

Київ 1999

Передмова

1 РОЗРОБЛЕНО Науково-дослідним інститутом автоматизованих систем в будівництві Державного комітету України у справах містобудування і архітектури

2 ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

3 ВВЕДЕНО ВПЕРШЕ

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту спеціальних
телекомунікаційних систем та захисту інформації
Служби безпеки України

від “ 28 ” травня 1999 року № 26

Технічний захист інформації на програмно-керованих АТС загального користування Специфікації гарантій захисту

НД ТЗІ 2.5-002-99

ДСТСЗІ СБ України

Київ

Зміст

1 Галузь використання 1

2 Нормативні посилання 2

3 Визначення, позначення і скорочення 2

4 Загальні положення 5

5 Специфікації гарантій безпеки середовища персоналу 5

6 Специфікації гарантій стандартизації технологічного середовища 10

7 Специфікації гарантій забезпечення спостережності та керованості технологічного середовища 12

8 8 Специфікації гарантій забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища 14

9 Специфікації гарантій якості документаці 16

НД ТЗІ 2.5-002-99

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

НА ПРОГРАМНО-КЕРОВАНИХ АТС ЗАГАЛЬНОГО КОРИСТУВАННЯ

СПЕЦИФІКАЦІЇ ГАРАНТІЙ ЗАХИСТУ

Чинний від 1999-07-01

1 Галузь використання

Цей нормативний документ (НД) установлює вимоги до гарантій захисту інформації, що циркулює на програмно-керованих АТС загального користування, а також на установських (відомчих, корпоративних) АТС.

Положення НД поширюються на програмно-керовані АТС (далі - АТС), у яких зберігається та циркулює інформація, що підлягає технічному захисту (див. ДСТУ 3396.0-96).

Вимоги НД не поширюються на захист:

- міжстанційних каналів синхронізації, сигналізації та передачі абонентської інформації;
- від зловмисних дій авторизованих користувачів у межах наданих їм повноважень, що наносять збиток власникам інформаційних ресурсів;
- елементів АТС від екстремізму і вандалізму авторизованих користувачів;
- телефонної мережі від некоректного вмикання в її структуру вперше запроваджуваних АТС або АТС, що модернізуються.

Захист елементів АТС від фізичного доступу, ушкоджень, розкрадань і підмін у цьому НД розглядається в загальному вигляді і лише як необхідна обмежувальна міра в процесі здійснення заходів щодо ТЗІ. Передбачається, що вжиті заходи щодо обмеження фізичного доступу до зони станційного устаткування достатні, щоб виключити можливість несанкціонованого доступу (НСД) в цю зону не уповноважених осіб.

Документ призначений для замовників, розроблювачів, виготовлювачів і постачальників АТС, операторів зв'язку національного, реґіонального і місцевого рівнів, юридичних осіб - власників і користувачів АТС, а також для організацій і підприємств, що здійснюють оцінку захищеності інформації на АТС від НСД, витоків і спеціальних впливів через технічні канали.

Вимоги цього НД є обов'язковими для підприємств, організацій, юридичних осіб, діючих на терені України незалежно від їх форм власності та відомчої підпорядкованості, які здійснюють діяльність, пов'язану з розробкою, виготовленням, експлуатацією АТС, а також проводять оцінку захищеності інформації на АТС від НСД, витоків та спеціальних впливів через технічні канали.

2 Нормативні посилання

У цьому нормативному документі ТЗІ використані посилання на такі нормативні документи:

- ДСТУ 3396.2-97 - Захист інформації. Технічний захист інформації. Терміни та визначення;
- НД ТЗІ 3.7-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова);
- НД ТЗІ 2.5-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;
- НД ТЗІ 2.7-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

3 Визначення, позначення і скорочення

У цьому документі використані терміни і визначення, що відповідають наведеним у ДСТУ 2615-94, ДСТУ 2621-94 і ДСТУ 3396.2-97.

Крім того, вводяться або уточнюються стосовно до АТС згідно з НД ТЗІ 1.1-001-99 нижченаведені терміни і визначення.

Інформаційний ресурс - це власне інформація або будь-який об'єкт, що є елементом певної інформаційної технології (технічні засоби обчислювальної або телекомунікаційної техніки, програми, дані і т. ін.).

Уразливість інформації - фундаментальна властивість інформації наражатися на небажані з точки зору її власників впливи з боку різного роду несприятливих чинників середовища існування інформаційних ресурсів;

ТЗІ на АТС - запобігання за допомогою інженерно-технічних заходів реалізаціям загроз для інформаційних ресурсів АТС, що створюються через технічні канали , через канали спеціальних впливів та шляхом несанкціонованого доступу.

Канали спеціальних впливів на елементи АТС - канали, через які впливи на технічні (апаратні) засоби АТС приводять до створення загроз для інформації.

Реалізація загроз для інформації на АТС через канали спеціальних впливів можлива з-за :

- кількісної недостатності компонентів АТС;
- якісної недостатності компонентів і (або) всієї АТС у цілому;
- навмисної або ненавмисної діяльності осіб, які, в свою чергу, впливають на елементи АТС з використанням програмних і (або) технічних засобів;
- несправностей апаратних елементів АТС;
- виходів за межі припустимих значень параметрів зовнішнього середовища функціонування АТС (у тому числі, пов'язаними зі стихійними лихами, катастрофами й іншими надзвичайними подіями);

- помилок і некоректних дій суб'єктів доступу до ресурсів АТС на стадії її промислової експлуатації.

Кількісна недостатність компонентів - фізична недостатність компонентів АТС, що не дозволяє забезпечити потрібну захищеність інформаційних ресурсів в розрізі розглянутих показників ефективності захисту.

Якісна недостатність - недосконалість архітектури чи структури АТС, організації технологічних процесів на АТС, проектних рішень на будь-якому з видів забезпечення АТС (програмного, апаратного, інформаційного і т. ін.), недоробки функціональних та принципових схем, конструкції компонентів і (або) всієї АТС у цілому, внаслідок чого не забезпечується потрібна захищеність інформаційних ресурсів у розрізі розглянутих показників ефективності захисту.

Відмова - порушення працездатності певного елемента АТС, що унеможвлює виконання ним своїх функцій.

Збій - тимчасове порушення працездатності певного елемента АТС, внаслідок чого з'являється можливість хибного виконання ним у цей момент своїх функцій.

Помилка - хибне (одноразове або систематичне) виконання елементом АТС однієї або кількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану.

Стихійне лихо - спонтанно виникаюче природне явище, що виявляється як могутня руйнівна сила.

Зловмисні дії - дії людей, що спеціально спрямовані на порушення захищеності інформаційних ресурсів.

Побічне явище - явище, що супроводжує виконання елементом АТС своїх основних функцій, внаслідок якого можливе порушення захищеності інформаційних ресурсів АТС.

Штатні засоби доступу (до інформаційних ресурсів АТС) - системні термінали, термінали обслуговування (у тому числі, віддалені), телефонні комутатори та абонентські прикінцеві пристрої.

Закладний пристрій - позаштатний технічний пристрій, встановлений і замаскований у апаратному середовищі АТС з метою реалізації загроз для інформації.

Програмна закладка - позаштатна комп'ютерна програма, встановлена і замаскована у програмному середовищі АТС з метою реалізації загроз для інформації.

Програмно-апаратні закладні пристрої (закладки) - закладні пристрої та (або) програмні закладки.

Модель порушника - опис ймовірних дій порушника, рівня його повноважень, ресурсних можливостей, використовуваних ним програмних і (або) апаратних засобів з метою реалізації загроз для інформації на АТС.

Модель загроз для інформації на АТС - опис способів і засобів здійснення суттєвих загроз для інформаційних ресурсів із зазначенням рівнів гранично припустимих втрат, що пов'язані з їхніми можливими проявами в конкретних або передбачуваних умовах застосування АТС.

Функціональна послуга захисту (ФПЗ) - взаємопов'язана множина виконуваних АТС елементарних функцій, яка дозволяє протистояти певним загрозам для інформації.

Засіб захисту - програмний і (або) технічний засіб, який безпосередньо реалізує певну ФПЗ.

Механізм захисту - процедура або частина процедури реалізації певної ФПЗ.

Стійкість (потужність) механізму захисту - його здатність протистояти прямим атакам, тобто спробам його безпосереднього злому.

Модель захисту - опис взаємопов'язаної множини ФПЗ із зазначенням необхідних рівнів стійкості реалізованих механізмів захисту, у випадку реалізації якої забезпечується потрібний рівень захисту інформації на АТС.

База захисту АТС - сукупність всіх елементів системи ТЗІ (методологічних, методичних, проектних, програмних, апаратних, організаційних і т.ін.), що мають відношення до організації протидії загрозам для інформаційних ресурсів на АТС.

Комплекс засобів і механізмів захисту (КЗМЗ) - взаємопов'язаний набір засобів і механізмів ТЗІ, що реалізують обрану модель захисту інформаційних ресурсів на АТС.

Гарантії захисту на певній стадії життєвого циклу АТС - сукупність вимог до реалізації організаційно-технічних заходів на цій стадії життєвого циклу АТС, що спрямовані на підвищення захищеності інформації на АТС.

Заявник - юридична або фізична особа, що є ініціатором проведення оцінювальних робіт;

Експерт - фізична особа, яка має високу кваліфікацію, спеціальні знання, безпосередньо здійснює експертизу і несе персональну відповідальність за достовірність та повноту аналізу, обгрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи.

Оцінка АТС за критеріями ТЗІ - комплекс спеціалізованих дослідницько-аналітичних та експериментальних робіт, що виконуються з метою визначення відповідності системи захисту інформації на АТС до вимог (специфікацій) нормативних документів з ТЗІ.

Експертиза АТС за критеріями ТЗІ - діяльність, метою якої є дослідження, перевірка, аналіз та оцінка науково-технічного рівня системи захисту інформації на АТС, а також підготовка обгрунтованих висновків для прийняття рішення щодо рівня захищеності інформаційних ресурсів АТС в описаних Заявником умовах експлуатації АТС та рівня довіри до результатів оцінки.

Критерії дієвості - нормуючі умови, вимоги і показники, згідно з якими оцінюється коректність системи ТЗІ на АТС.

Довірчі критерії - нормуючі умови, вимоги і показники, згідно з якими оцінюється рівень довіри до коректності реалізації системи ТЗІ на АТС.

Оцінка ефективності системи ТЗІ на АТС - оцінка ступеня досконалості системи ТЗІ, що створена на АТС, стосовно "слабких місць" та "виломів" у захисті.

4 Загальні положення

4.1 У цьому документі надані специфікації гарантій захисту інформаційних ресурсів технологічних середовищ створення та експлуатації АТС.

Специфікації гарантій захисту необхідні для визначення рівнів довіри до коректності розробок, реалізацій та експлуатації систем ТЗІ на оцінюваних АТС.

4.2 Передбачається, що оцінка рівнів довіри виконується відповідно до базової методики оцінки захищеності інформації на АТС (див. НД ТЗІ 3.7-002-99), яка заснована на єдиних (уніфікованих) для Європейського Союзу "Критеріях оцінки безпеки систем інформаційної техніки - ITSEC".

4.3 У цьому документі специфіковані гарантії за п'ятьма аспектами забезпечення захищеності інформації в технологічному середовищі створення та експлуатації систем ТЗІ і АТС у цілому:

- гарантії безпеки середовища персоналу;
- гарантії стандартизації технологічного середовища;
- гарантії забезпечення спостережності і керованості технологічного середовища;
- гарантії забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища;
- гарантії якості документації.

5 Специфікації гарантій безпеки середовища персоналу

5.1 Для забезпечення гарантій безпеки середовища персоналу, тобто для забезпечення визначеного рівня довіри до персоналу, необхідно виконати вимоги, основні види яких наведені в таблиці 5.1.

Таблиця 5.1

Види вимог до безпеки середовищ персоналу	Позначення виду вимог
1 Вимоги до системи організації праці	Т1.1
2 Вимоги до контролю системи організації праці	Т1.2
3 Вимоги до поведінки персоналу в робочий час	Т1.3
4 Вимоги до контролю поведінки персонала в робочий час	Т1.4
5 Вимоги до поведінки персоналу в неробочий час	Т1.5
6 Вимоги до контролю поведінки персонала в неробочий час	Т1.6

5.2. Специфікації вимог до безпеки середовища персоналу наведені в таблицях 5.2 - 5.7

Таблиця 5.2

Вимоги до системи організації праці	Позначення вимог
1 Забезпечення відповідності кваліфікації персоналу змісту виконуваних робіт	Т1.1.1
2 Наявність системи підвищення кваліфікації	Т1.1.2
3 Наявність системи в доборі кадрів	Т1.1.3
4 Наявність системи розподілу повноважень (посадових прав і обов'язків)	Т1.1.4
5 Дотримування принципу мінімальної достатності знань персоналу про об'єкти, що охоплені захистом (зокрема, наявність системи категоризації допуску до інформації, приміщення і т.ін.)	Т1.1.5
6 Наявність системи заохочення і покарання	Т1.1.6
7 Наявність умов для роботи з секретною інформацією за другою формою допуску	Т1.1.7
8 Наявність умов для роботи з секретною інформацією за першою формою допуску	Т1.1.8
9 Наявність системи оцінки якості праці	Т1.1.9
10 Наявність естетичних і психологічних чинників стимулювання праці	Т1.1.10
11 Наявність корпоративних етичних норм поведінки в процесі праці	Т1.1.11
12 Наявність суспільних (моральних) стимулів до праці і до захисту корпоративних (зокрема, державних) інтересів	Т1.1.12

Таблиця 5.3

Вимоги до контролю системи організації праці	Позначення вимог
1 Періодичний і (або) вибірковий контроль кваліфікації персоналу	Т1.2.1
2 Постійний контроль кваліфікації персоналу	Т1.2.2
3 Періодичний аналіз системи підвищення кваліфікації персоналу	Т1.2.3
4 Періодичний контроль системи підвищення кваліфікації персоналу	Т1.2.4
5 Постійний аналіз системи підвищення кваліфікації персоналу	Т1.2.5
6 Постійний контроль системи підвищення кваліфікації персоналу	Т1.2.6
7 Періодичний і (або) вибірковий аналіз якості добору персоналу	Т1.2.7
8 Постійний аналіз якості добору персоналу	Т1.2.8
9 Періодичний аналіз системи в доборі кадрів	Т1.2.9
10 Постійний аналіз системи в доборі кадрів	Т1.2.10
11 Періодичний аналіз розподілу повноважень (посадових прав і обов'язків) персоналу	Т1.2.11
12 Постійний аналіз розподілу повноважень персоналу	Т1.2.12
13 Періодичний аналіз системи розподілу повноважень	Т1.2.13
14 Постійний аналіз системи розподілу повноважень	Т1.2.14
15 Періодичний і (або) вибірковий контроль дотримання персоналом посадових прав і обов'язків	Т1.2.15
16 Постійний контроль дотримання персоналом посадових прав і обов'язків	Т1.2.16
17 Періодичний аналіз системи, що реалізує принцип мінімальної достатності знань персонала про об'єкти, що охоплені захистом зокрема, аналіз системи категорізації допуска персоналу до інформації, до приміщень, до технологічного устаткування і т.інш.)	Т1.2.17
18 Постійний аналіз системи, що реалізує принцип мінімальної достатності знань персонала про об'єкти, що охоплені захистом	Т1.2.18

Закінчення таблиці 5.3

Вимоги до контролю системи організації праці	Позначення вимог
19 Періодичний аналіз системи заохочення і покарання	Т1.2.19
20 Постійний аналіз системи заохочення і по карання	Т1.2.20
21 Періодичний і (або) вибірковий контроль коректності реалізації адміністрацією прийнятої системи заохочення і покарання	Т1.2.21
22 Постійний контроль коректності реалізації адміністрацією прийнятої системи заохочення і покарання	Т1.2.22
23 Наявність режимного органу	Т1.2.23
24 Періодичний контроль умов роботи з секретною інформацією	Т1.2.24
25 Постійний контроль умов роботи із секретною інформацією	Т1.2.25
26 Постійний контроль роботи персоналу з секретною інформацією	Т1.2.26
27 Безперервний і безпосередній контроль роботи персоналу із секретною інформацією	Т1.2.27
28 Періодичний аналіз системи роботи із секретною інформацією	Т1.2.28
29 Постійний аналіз системи роботи із секретной інформацією	Т1.2.29
30 Періодичний аналіз системи оцінки якості праці	Т1.2.30
31 Постійний аналіз системи оцінки якості праці	Т1.2.31
32 Періодичний і (або) вибірковий контроль оцінки якості праці персоналу	Т1.2.32
33 Постійний контроль оцінки якості праці персонала	Т1.2.33
34 Періодичний аналіз естетичних і психологічних чинників стимулювання праці	Т1.2.34
35 Постійний аналіз естетичних і психологічних чинників стимулювання праці	Т1.2.35
36 Періодичний аналіз корпоративних етичних норм поведінки в процесі праці	Т1.2.36
37 Постійний аналіз корпоративних етичних норм поведінки в процесі праці	Т1.2.37
38 Періодичний аналіз суспільних (моральних)стимулів до праці і захисту корпоративних інтересів	Т1.2.38
39 Постійний аналіз суспільних (моральних) стимулів до праці і захисту корпоративних интересів	Т1.2.39
40 Наявність служби контролю системи організації праці	Т1.2.40
41 Постійний і безпосередній контроль усіх ланок системи організації праці	Т1.2.41

Таблиця 5.4

Вимоги до поведінки персоналу в робочий час	Позначення вимог
1 Підтримка загальної дисципліни праці	Т1.3.1
2 Дотримування технологічної дисципліни	Т1.3.2
3 Виконання правил роботи із секретною інформацією	Т1.3.3
4 Дотримування режиму конфіденційності	Т1.3.4.
5 Виконання режимних обмежень (зокрема, щодо фізичних переміщень документації, матеріальних потоків, суб'єктів і т.ін.) у процесі праці	Т1.3.5

Таблиця 5.5

Вимоги до контролю поведінки персоналу в робочий час	Позначення вимог
1 Наявність обліку робочого часу персоналу	Т1.4.1
2 Періодичний або (і) вибірковий контроль дотримання технологічної дисципліни	Т1.4.2
3 Постійний контроль дотримання технологічної дисципліни	Т1.4.3
4 Періодичний або вибірковий контроль поведінки персоналу в робочий час	Т1.4.4
5 Постійний і безпосередній контроль поведінки персоналу в робочий час	Т1.4.5

Таблиця 5.6

Вимоги до поведінки персоналу в неробочий час	Позначення вимог
1 Пред'явлення достовірних анкетних даних та документів на рівні вимог трудового законодавства	Т1.5.1
2 Відсутність фактів антигромадської поведінки	Т1.5.2
3 Відсутність аномалій у психофізіологичному стані організму та у рівні залежності від суспільно шкідливих звичок (алкоголю, наркотиків і т.ін.)	Т1.5.3
4 Дотримування зобов'язань, узятих при оформленні допуску до роботи із секретними документами	Т1.5.4
5 Виконання обмежувальних умов поведінки у неробочий час	Т1.5.5
6 Дотримування режимних умов у вільний від роботи час	Т1.5.6

Таблиця 5.7

Вимоги до контролю поведінки персонала у неробочий час	Позначення вимог
1 Систематизований облік і періодичний контроль вірогідності даних про персонал	Т1.6.1
2 Систематизований облік і постійний контроль вірогідності даних про персонал	Т1.6.2
3 Періодичний або вибірковий контроль поведінки персоналу в неробочий час	Т1.6.3
4 Постійний контроль поведінки персоналу в неробочий час (наприклад, за рахунок введения казарменого положення для персоналу - військових і т.ін.)	Т1.6.4
5 Періодичні перевірки стана здоров'я персоналу	Т1.6.5
6 Постійний контроль стана здоров'я персоналу	Т1.6.6

5.3 Специфікації рівнів довіри до персоналу наведені в таблиці 5.8.

Таблиця 5.8

Рівні довіри до персоналу	Вимоги до безпеки середовища персоналу					
	Т1.1	**Т1.2**	**Т1.3**	**Т1.4**	**Т1.5**	**Т1.6**
1 Г (УБПі-0) (нульовий рівень довіри)	Т1.1.1 Т1.1.6	-	-	-	-	-
2 Г (УБПі-1) (перший рівень довіри)	Т1.1.1 Т1.1.3 Т1.1.4 Т1.1.6	Т1.2.1 Т1.2.7 Т1.2.11 Т1.2.15	Т1.3.1 Т1.3.2	Т1.4.1 Т1.4.2	Т1.5.1 Т1.5.2	Т1.6.1

Продовження таблиці 5.8

Рівні довіри до персоналу	**Вимоги до безпеки середовища персоналу**					
	Т1.1	**Т1.2**	**Т1.3**	**Т1.4**	**Т1.5**	**Т1.6**
3 Г (УБПі-2) (другий рівень довіри)	Т1.1.1 Т1.1.2 Т1.1.3 Т1.1.4 Т1.1.6 Т1.1.7	Т1.2.2 Т1.2.3 Т1.2.4 Т1.2.7 Т1.2.9 Т1.2.11 Т1.2.13 Т1.2.15 Т1.2.19 Т1.2.21 Т1.2.23 Т1.2.24 Т1.2.26 Т1.2.28 Т1.2.40	Т1.3.1 Т1.3.2 Т1.3.3 Т1.3.4	Т1.4.1 Т1.4.3 Т1.4.4	Т1.5.1 Т1.5.2 Т1.5.3 Т1.5.4	Т1.6.2 Т1.6.3 Т1.6.5
4 Г (УБПі-3) (третій рівень довіри)	Т1.1.1 Т1.1.2 Т1.1.3 Т1.1.4 Т1.1.5 Т1.1.6 Т1.1.7 Т1.1.8 Т1.1.9 Т1.1.10 Т1.1.11 Т1.1.12	Т1.2.2 Т1.2.5 Т1.2.6 Т1.2.8 Т1.2.10 Т1.2.12 Т1.2.14 Т1.2.16 Т1.2.17 Т1.2.20 Т1.2.22 Т1.2.23 Т1.2.25 Т1.2.26 Т1.2.27 Т1.2.29 Т1.2.30 Т1.2.32 Т1.2.34 Т1.2.36 Т1.2.38 Т1.2.40	Т1.3.1 Т1.3.2 Т1.3.3 Т1.3.4 Т1.3.5	Т1.4.1 Т1.4.3 Т1.4.5	Т1.5.1 Т1.5.2 Т1.5.3 Т1.5.4 Т1.5.5	Т1.6.2 Т1.6.4 Т1.6.6

Закінчення таблиці 5.8

Рівні довіри до персоналу	Вимоги до безпеки середовища персоналу					
	Т1.1	**Т1.2**	**Т1.3**	**Т1.4**	**Т1.5**	**Т1.6**
5 Г (УБПі-4) (четвертий рівень довіри)	Т1.1.1 Т1.1.2 Т1.1.3 Т1.1.4 Т1.1.5 Т1.1.6 Т1.1.7 Т1.1.8 Т1.1.9 Т1.1.10 Т1.1.11 Т1.1.12	Т1.2.2 Т1.2.5 Т1.2.6 Т1.2.8 Т1.2.10 Т1.2.12 Т1.2.14 Т1.2.16 Т1.2.18 Т1.2.20 Т1.2.22 Т1.2.23 Т1.2.25 Т1.2.26 Т1.2.27 Т1.2.29 Т1.2.31 Т1.2.33 Т1.2.35 Т1.2.37 Т1.2.39 Т1.2.40 Т1.2.41	Т1.3.1 Т1.3.2 Т1.3.3 Т1.3.4 Т1.3.5	Т1.4.1 Т1.4.3 Т1.4.5	Т1.5.1 Т1.5.2 Т1.5.3 Т1.5.4 Т1.5.5 Т1.5.6	Т1.6.2 Т1.6.4 Т1.6.6

Примітка: Убпі - мнемонічне позначення логічного об'єкта безпеки в і-му середовищі персоналу.

6 Специфікації гарантій стандартизації технологічного середовища

6.1 Для одержання гарантій забезпечення якості стандартизації технологічного середовища необхідно виконати вимоги, основні види яких наведені таблиці 6.1.

Таблиця 6.1

Види вимог до стандартизації середовища	Позначення виду вимог
1 Вимоги до повноти охоплення стандартами елементів середовища	Т3.1
2 Вимоги до глибини охоплення стандартами технологій роботи в середовищі	Т3.2
3 Вимоги до рівня значущості стандартів (міждержавні, державні, галузеві, стандарти підприємств)	Т3.3
4 Вимоги до рівня взаємоузгодженості (гармонізованості)стандартів	Т3.4

6.2 Вимоги до стандартизації технологічного середовища наведені в таблицях 6.2 - 6.5.

Жорсткість вимог до якості стандартизації зростає в міру збільшення порядкових номерів вимог у рамках таблиць 6.2 - 6.5.

Таблиця 6.2

Вимоги до повноти охоплення стандартами елементів технологічного середовища	**Позначення вимог**
1 Стандартизація окремих елементів середовища	Т3.1.1
2 Стандартизація критично важливих елементів середовища	Т3.1.2
3 Повна стандартизація всіх основних підсистем середовища	Т3.1.3
4 Повна стандартизація всіх елементів середовища	Т3.1.4

Таблиця 6.3

Вимоги до глибини охоплення стандартами технологій роботи в середовищі	**Позначення вимог**
1 Низький рівень глибини охоплення стандартами технологій роботи в середовищі	Т3.2.1
2 Середній рівень глибини охоплення стандартами технологій роботи в середовищі	Т3.2.2
3 Високий рівень глибини охоплення стандартами технологій роботи в середовищі	Т3.2.3

Таблиця 6.4

Вимоги до рівня значущості стандартів	**Позначення вимог**
1 Стандарти підприємства	Т3.3.1
2 Галузеві стандарти	Т3.3.2
3 Державні стандарти	Т3.3.3
4 Міждержавні стандарти	Т3.3.4

Таблиця 6.5

Вимоги до рівня взаємоузгодженості стандартів	**Позначення вимог**
1 Часткова взаємоузгодженість стандартів за специфікаціями основних елементів середовища	Т3.4.1
2 Повна взаємоузгодженість стандартів за специфікаціями основних елементів середовища	Т3.4.2
3 Повна взаємоузгодженість стандартів за специфікаціями всіх елементів середовища	Т3.4.3
4 Відповідність формально затвердженому профилю стандартів середовища (наприклад, відповідність державному профілю стандартів середовищ)	Т3.4.4

6.3 Специфікації рівнів гарантій якості стандартизації середовища наведені в таблиці 6.6.

Таблиця 6.6

Рівні гарантій якості стандартизації середовища	**Вимоги до якості стандартизації середовища**			
	Т3.1	**Т3.2**	**Т3.3**	**Т3.4**
1 Г (УССі-0) (нульовий рівень гарантій)	Т3.1.1	Т3.2.1	Т3.3.1	Т3.4.1
2 Г (УССі-1) (перший рівень гарантій)	Т3.1.2	Т3.2.2	Т3.3.2	Т3.4.2
3 Г (УССі-2) (другий рівень гарантій)	Т3.1.3	Т3.2.3	Т3.3.3	Т3.4.2
4 Г (УССі-3) (третій рівень гарантій)	Т3.1.4	Т3.2.3	Т3.3.4	Т3.4.3
5 Г (УССі-4) (четвертий рівень гарантій)	Т3.1.4	Т3.2.3	Т3.3.4	Т3.4.4

Примітка. Уссі - мнемонічне позначення логічного об'єкта стандартизації і-го технологічного середовища.

7 Специфікації гарантій забезпечення спостережності та керованості технологічного середовища

7.1 Для одержання гарантій забезпечення спостережності і керованості технологічного середовища необхідно виконати вимоги, основні види яких наведені в таблиці 7.1.

Таблиця 7.1

Види вимог до спостережності та керованості технологічного середовища	**Позначення виду вимог**
1 Вимоги до ефективності аудіту (контрольованості) технологічного середовища	Т6.1
2 Вимоги до автентифікації (суб'єктів) та ідентифікації об'єктів (процесів, ресурсів) у технологічному середовищі	Т6.2
3 Вимоги до сертифікованих (достовірних) шляхів	Т6.3
4 Вимоги до керованості технологічного середовища	Т6.4

7.2 Вимоги до спостережності і керованості технологічного середовища наведені в таблицях 7.2 - 7.5.

Жорсткість вимог до якості спостережності і керованості середовища зростає в міру збільшення порядкових номерів вимог у рамках таблиць 7.2 - 7.5.

Таблиця 7.2

Вимоги до ефективності аудиту технологічного середовища	**Позначення вимог**
1 Нерегулярний у часі спорадичний аудіт	Т6.1.1
2 Регулярний періодичний аудіт	Т6.1.2
3 Безперервний у часі постійний аудіт	Т6.1.3
4 Частковий (з точки зору повноти охоплення аудітом суб'єктів, процесів і ресурсів) вибірковий аудіт	Т6.1.4
5 Повний аудіт критично важливих елементів технологічного середовища при вибірковому аудиті всіх інших елементів середовища	Т6.1.5
6 Повний аудіт всіх елементів технологічного середовища	Т6.1.6
7 Низький рівень захищеності механізмів аудіта	Т6.1.7
8 Середній рівень захищеності механізмів аудіта	Т6.1.8
9 Високий рівень захищеності механізмів аудіта	Т6.1.9

Таблиця 7.3

Вимоги до автентифікації суб'єктів та ідентифікації об'єктів(процесів, ресурсів)	Позначення вимог
1 Нерегулярна (у часі) спорадична автентифікація й ідентифікація об'єктів та суб'єктів технологічного середовища	Т6.2.1
2 Регулярна періодична автентифікація та ідентифікація суб'єктів і об'єктів технологічного середовища	Т6.2.2
3 Неперервна (у часі) постійна автентифікація та ідентифікація суб'єктів і об'єктів технологічного середовища	Т6.2.3
4 Часткова (з точки зору повноти охоплення) вибіркова автентифікація й ідентифікація суб'єктов і об'єктів технологічного середовища	Т6.2.4
5 Автентифікація та ідентифікація усіх критически важливих суб'єктів і об'єктів середовища	Т6.2.5
6 Автентифікація й ідентифікація усіх суб'єктів і об'єктів технологічного середовища	Т6.2.6
7 Низький рівень захищеності механізмів автентифікації й ідентифікації	Т6.2.7
8 Середній рівень захищеності механізмів автентифікації й ідентифікації	Т6.2.8
9 Високий рівень захищеності механізмів автентифікації й ідентифікації	Т6.2.9

Таблиця 7.4

Вимоги до сертифікованих (достовірних) шляхів	Позначення вимог
1 Часткова (з точки зору повноти охоплення елементів середовища) сертифікованість шляхів в технологічному середовищі	Т6.3.1
2 Сертифікованість шляхів у критично важливих елементах технологічного середовища	Т6.3.2
3 Повна сертифікованість шляхів у технологічному середовищі	Т6.3.3

Таблиця 7.5

Вимоги до керованості технологічного середовища	Позначення вимог
1 Нерегулярна (у часі) спорадична керованість технологічного середовища	Т6.4.1
2 Регулярна періодична керованість технологічного середовища	Т6.4.2
3 Неперервна (у часі) постійна керованість технологічного середовища	Т6.4.3
4 Часткова (з точки зору повноти охоплення елементів середовища) вибіркова керованість технологічного середовища	Т6.4.4
5 Керованість усіх критично важливих елементів технологічного середовища	Т6.4.5
6 Повна керованість всіх елементів технологічного середовища	Т6.4.6
7 Низький рівень захищеності механізмів керування середовищем	Т6.4.7
8 Середній рівень захищеності механізмів керування середовищем	Т6.4.8
9 Високий рівень захищеності механізмів керування середовищем	Т6.4.9

7.3 Специфікації рівнів гарантій спостережності та керованості технологічного середовища наведені в таблиці 7.6.

Таблиця 7.6

Рівні гарантій спостережності та керованості технологічного середовища	Вимоги до спостережності і керованості технологічного середовища			
	Т6.1	**Т6.2**	**Т6.3**	**Т6.4**
1 УБ6$_i$- 0 (нульовий рівень гарантій)	Т6.1.1 Т6.1.4	-	-	Т6.4.1 Т6.4.4
2 УБ6$_i$ – 1 (перший рівень гарантій)	Т6.1.2 Т6.1.4 Т6.1.7	Т6.2.2 Т6.2.4 Т6.2.7	-	Т6.4.2 Т6.4.4 Т6.4.7
3 УБ6$_i$ – 2 (другий рівень гарантій)	Т6.1.2 Т6.1.5 Т6.1.7	Т6.2.2 Т6.2.5 Т6.2.7	Т6.3.1	Т6.4.2 Т6.4.5 Т6.4.7
4 УБ6$_i$ – 3 (третій рівень гарантій)	Т6.1.3 Т6.1.5 Т6.1.8	Т6.2.3 Т6.2.5 Т6.2.8	Т6.3.2	Т6.4.3 Т6.4.5 Т6.4.8
5 УБ6$_i$ – 4 (четвертий рівень гарантій)	Т6.1.3 Т6.1.6 Т6.1.9	Т6.2.3 Т6.2.6 Т6.2.9	Т6.3.3	Т6.4.3 Т6.4.6 Т6.4.9

Примітка: УБ6і - мнемонічне позначення логічного об'єкта спостережності і керованості і - го технологічного середовища.

8 Специфікації гарантій забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища

8.1 Для одержання гарантій забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища необхідно виконати вимоги, основні види яких наведені в таблиці 8.1.

Таблиця 8.1

Види вимог до забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища	Позначення виду вимог
1 Вимоги до реалізації правил розподілу доступу	Т4.1
2 Вимоги до реалізації послуг повторного використання об'єктів	Т4.2
3 Вимоги до захищеності від схованих каналів витоку і спеціальних впливів на елементи АТС	Т4.3
4 Вимоги до фізичної цілісності	Т4.4
5 Вимоги до реалізації послуг відкоту	Т4.5
6 Вимоги до розмежування обов'язків	Т4.6
7 Вимоги до самотестуванню об'єктів	Т4.7

8.2 Вимоги до конфіденційності і цілісності інформаційних ресурсів технологічного середовища наведені в таблиці 8.2.

Таблиця 8.2

Вимоги до конфіденційності і цілісності інформаційних ресурсів середовища	**Позначення вимоги**
1 Нерегулярне (у часі)спорадичне забезпечення послугами захисту від порушень конфіденційності і цілісності	Т4.1.1; Т4.2.1; Т4.3.1; Т4.4.1; Т4.5.1; Т4.6.1; Т4.7.1
2 Регулярне періодичне забезпечення послугами захисту від порушень конфіденційності і цілісності	Т4.1.2; Т4.2.2; Т4.3.2; Т4.4.2; Т4.5.2; Т4.6.2; Т4.7.2
3 Безперервне (у часі) постійне забезпечення послугами захисту від порушень конфіденційності і цілісності	Т4.1.3; Т4.2.3; Т4.3.3; Т4.4.3; Т4.5.3; Т4.6.3; Т4.7.3
4 Часткове (вибіркове) забезпечення (з точки зору повноти охоплення елементів середовища) послугами захисту	Т4.1.4; Т4.2.4; Т4.3.4; Т4.4.4; Т4.5.4; Т4.6.4; Т4.7.4
5 Забезпечення послугами захисту в просторі всіх критично важливих суб'єктів і об'єктів середовища	Т4.1.5; Т4.2.5; Т4.3.5; Т4.4.5; Т4.5.5; Т4.6.5; Т4.7.5
6 Забезпечення повного охоплення усіх елементів середовища послугами захисту від порушень конфіденційності і цілісності	Т4.1.6; Т4.2.6; Т4.3.6; Т4.4.6; Т4.5.6; Т4.6.6; Т4.7.6
7 Забезпечення базового (мінімального) рівня захищеності механізмів захисту у разі реалізації послуг захисту технологічного середовища від порушень конфіденційності і цілісності	Т4.1.7; Т4.2.7; Т4.3.7; Т4.4.7; Т4.5.7; Т4.6.7; Т4.7.7
8 Забезпечення середнього рівня захищеності механізмів захисту у разі реалізації послуг захисту від порушень конфіденційності і цілісності	Т4.1.8; Т4.2.8; Т4.3.8; Т4.4.8; Т4.5.8; Т4.6.8; Т4.7.8
9 Забезпечення високого рівня захищеності механізмів захисту у разі реалізації послуг захисту від порушень конфіденційності і цілісності	Т4.1.9; Т4.2.9; Т4.3.9; Т4.4.9; Т4.5.9; Т4.6.9; Т4.7.9

8.3. Специфікації рівнів гарантій конфіденційності і цілісності інформаційних ресурсів у технологічному середовищі наведені в таблиці 8.3.

Таблиця 8.3

Рівні гарантій конфіденційності і цілісності інформаційних ресурсів у технологічному середовищі	**Вимоги до конфіденційності та цілісності інформаційних ресурсів середовища**
1 УБ4$_i$ – 0 (нульовий рівень гарантій)	Т4.1.1; Т4.4.1; Т4.6.1; Т4.1.4; Т4.4.4; Т4.6.4; Т4.1.7; Т4.4.7; Т4.6.7
2 УБ4$_i$ – 1 (перший рівень гарантій)	Т4.1.2; Т4.4.2; Т4.6.2; Т4.1.5; Т4.4.5; Т4.6.5; Т4.1.8; Т4.4.8; Т4.6.8
3 УБ4$_i$ – 2 (другий рівень гарантій)	Т4.1.3; Т4.2.2; Т4.3.2; Т4.4.3; Т4.5.2; Т4.6.3; Т4.7.2; Т4.1.6; Т4.2.5; Т4.3.5; Т4.4.6; Т4.5.5; Т4.6.6; Т4.7.5; Т4.1.9; Т4.2.8; Т4.3.8; Т4.4.9; Т4.5.8; Т4.6.9; Т4.7.8
4 УБ4$_i$ – 3 (третій рівень гарантій)	Т4.1.3; Т4.2.3; Т4.3.3; Т4.4.3; Т4.5.3; Т4.6.3; Т4.7.3; Т4.1.6; Т4.2.6; Т4.3.6; Т4.4.6; Т4.5.6; Т4.6.6; Т4.7.6; Т4.1.9; Т4.2.9; Т4.3.9; Т4.4.9; Т4.5.9; Т4.6.9; Т4.7.9

Примітка: УБ4і - мнемонічне позначення логічного об'єкта забезпечення конфіденційності і цілісності інформаційних ресурсів в і-му технологічному середовищі.

9 Специфікації гарантій якості документації

9.1 Для забезпечення гарантій якості документації необхідно виконати вимоги, основні види яких наведені в таблиці 9.1.

Таблиця 9.1

Види вимог до якості документації	Позначення виду вимог
1 Вимоги до повноти документації (до рівня охоплення документацією елементів середовища)	Т2.1
2 Вимоги до рівня деталізації опису середовища і (або) технологій	Т2.2
3 Вимоги до вірогідності інформації, що міститься в документації	Т2.3
4 Вимоги до якості оформлення документації	Т2.4

9.2 Вимоги до якості документації наведені в таблицях 9.2 - 9.5.

Жорсткість вимог до якості документації зростає в міру збільшення порядкових номерів вимог у рамках таблиць 9.2 - 9.5.

Таблиця 9.2

Вимоги до повноти документації	Позначення вимог
1 Охоплення документацією окремих елементів середовища і (або) технологій	Т2.1.1
2 Охоплення документацією критично важливих елементів середовища і (або) технології	Т2.1.2
3 Охоплення документацією всіх основних підсистем середовищ і (або) технологій	Т2.1.3
4 Повне охоплення документацією усіх елементів середовища і технологій	Т2.1.4

Таблиця 9.3

Вимоги до рівня деталізації опису середовища і (або) технологій	Позначення вимог
1 Опис загальних характеристик елементів середовища і (або) технологій	Т2.2.1
2 Опис середовища і (або) технологій на рівні структурних схем і узагальнених алгоритмів роботи	Т2.2.2
3 Опис середовища і (або) технологій на рівні функціональних схем і детальних алгоритмів роботи	Т2.2.3
4 Детальний опис середовища і (або) технологій на рівні принципових схем, програм ЕОМ, інструкцій з експлуатації	Т2.2.4

Таблиця 9.4

Вимоги до вірогідності інформації, що міститься в документації	**Позначення вимоги**
1 Не більш однієї граматичної помилки на одну сторінку машинописного тексту	Т2.3.1
2 Не більш однієї граматичної помилки на десять сторінок машинописного тексту	Т2.3.2
3 Відсутність перекручувань змісту, що описують процеси (відсутність семантичних по милок)	Т2.3.3
4 Відсутність помилок у числових даних, найменуваннях ідентифікаторів, текстах програм для ЕОМ	Т2.3.4

Таблиця 9.5

Вимоги до якості оформлення документації	**Позначення вимог**
1 Оформлення відповідно до вимог нормативних документів	Т2.4.1

9.3 Специфікації рівнів гарантій якості документації наведені в таблиці 9.6.

Таблица 9.6

Рівні гарантій якості документації	Вимоги до якості документації			
	Т2.1	Т2.2	Т2.3	Т2.4
1 Г (УКДі-0) (нульовий рівень гарантій)	Т2.1.1	Т2.2.1	Т2.3.1	-
2 Г (УКДі-1) (перший рівень гарантій)	Т2.1.2	Т2.2.2	Т2.3.1	Т2.4.1
3 Г (УКДі-2) (другий рівень гарантій)	Т2.1.3	Т2.2.3	Т2.3.1 Т2.3.3	Т2.4.1
4 Г (УКДі-3) (третій рівень гарантій)	Т2.1.4	Т2.2.4	Т2.3.2 Т2.3.3	Т2.4.1
5 Г (УКДі-4) (четвертий рівень гарантій)	Т2.1.4	Т2.2.4	Т2.3.2 Т2.3.3 Т2.3.4	Т2.4.1

Примітка: Укді - мнемонічне позначення логічного об'єкта документованості в і-му технологічному середовищі.