НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Технічний захист інформації на програмно-керованих АТС загального користування

Специфікації функціональних послуг захисту

Департамент спеціальних телекомунікаційних систем
та захисту інформації Служби безпеки України

Київ 1999

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 функціональних послуг захисту

НД ТЗІ 2.5 – 001 – 99

ДСТСЗІ СБ України

Київ

Передмова

1 РОЗРОБЛЕНО Науково-дослідним інститутом автоматизованих систем в будівництві Державного комітету України у справах містобудування і архітектури (НДІАСБ) та Науково-виробничим об‘єднанням ІНТЕЛЕКТРОН

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

3 ВВЕДЕНО ВПЕРШЕ

Зміст

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ПРОГРАМНО-КЕРОВАНИХ АТС ЗАГАЛЬНОГО КОРИСТУВАННЯ. СПЕЦИФІКАЦІЇ ФУНКЦІОНАЛЬНИХ ПОСЛУГ ЗАХИСТУ.

Чинний від 1999-07-01

1 Галузь використання

Цей нормативний документ (НД) містить специфікації функціональних послуг захисту (ФПЗ) інформаційних ресурсів АТС, а також специфікації рівнів стійкості механізмів захисту інформації, які ці ФПЗ реалізують.

Дія цього документу поширюється на програмно-керовані АТС, що функціонують на мережі електрозв'язку загального користування, а також у складі відомчих (корпоративних, установських) проводових телефонних мереж, у яких зберігається та циркулює інформація, що підлягає технічному захисту (далі – АТС) (див. ДСТУ 3396.0-96 і НД ТЗІ 1.1-001-99).

Спецікації ФПЗ для АТС, що наведені в цьому документі, є нормами, які спрямовані на розв'язання таких задач:

– створення та оцінка захищених АТС за критеріями ТЗІ;

– створення та оцінка систем і засобів ТЗІ на АТС за критеріями ТЗІ;

– контроль рівня захищеності інформаційних ресурсів на АТС від ураження через технічні канали.

Цим документом необхідно керуватись згідно з НД ТЗІ 2.7-001-99 на стадіях розробки та реалізації техно-робочого проекту системи ТЗІ для АТС, а також на стадії оцінки АТС за критеріями ТЗІ.

Дія цього документу не поширюється 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 запроваджених АТС або АТС, що модернізуються.

Захист елементів АТС від фізичного доступу, ушкоджень, розкрадань і підмін у цьому НД розглядається у загальному вигляді і лише як необхідна обмежувальна міра під час 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 неуповноважених осіб.

Документ призначений для замовників, розроблювачів, виготовлювачів і постачальників АТС, операторів мереж електрозв'язку загального користування національного, регіонального і місцевого рівнів, юридичних осіб – власників і користувачів АТС, а також 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 НД ТЗІ використані посилання на такі нормативні документи:

– ДСТУ 2615-94 – Зв'язок телефонний. Загальні поняття. Телефонні мережі. Терміни та визначення;

– ДСТУ 2621-94 – Електрозв'язок. Зв'язок цифровий та системи передачі цифрові. Терміни та визначення;

– ДСТУ 3396.2-97 – Захист інформації. Технічний захист інформації. Терміни та визначення;

– НД ТЗІ 1.1-001-99 – Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення;

– НД ТЗІ 2.3-001-99 – Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова);

– НД ТЗІ 2.5-002-99 – Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій 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 3396.2-97, ДСТУ 2615-94 та ДСТУ 2621-94.

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 і (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 витоку інформації, через канали спеціальних впливів та шляхом несанкціонованого доступу.

Канали спеціальних впливів на елементи АТС – канали, через які впливи на технічні (апаратні) засоби АТС призводять до створення та здійснення 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) усієї АТС у цілому;

– навмисної або ненавмисної діяльності осіб, які, в свою чергу, впливають на елементи АТС із використанням програмних і (або) технічних засобів;

– несправностей апаратних елементів АТС;

– виходів за межі припустимих значень параметрів зовнішнього середовища (у тому числі, пов'язаними зі стихійними лихами, катастрофами та 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 необхідний рівень захищеності інформаційних ресурсів у розрізі розглянутих показників ефективності захисту.

Якісна недостатність – недосконаліть архітектури чи структури АТС, організації технологічних процесів на АТС, проектних рішень на будь-якому із видів забезпечення АТС (програмного, апаратного, інформаційного і т. ін.), недоробки функціональних або принципових схем, конструкції компонентів і (або) усієї АТС у цілому, внаслідок чого не забезпечується необхідний рівень захищеності інформаційних ресурсів у розрізі розглянутих показників ефективності захисту.

Відмова – порушення працездатності певного елемента АТС, що унеможливлює 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 певної системи своїх основних функцій, внаслідок якого можливе порушення захищеності інформаційних ресурсів на 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) технічних засобів, з метою реалізації загроз для інформації на АТС.

Модель загроз для інформації на АТС – опис сукупності суттєвих загроз для інформаційних ресурсів, способів і засобів їх здійснення із зазначенням рівнів гранично припустимих втрат, що пов'язані із 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, апраратних, 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.

Сертифікований канал можливої реалізації загроз для інформаційних ресурсів – стандартизований потенційно можливий документально зафіксований у моделях порушників спосіб (метод і (або) механізм) реалізації загроз для інформаційних ресурсів.

Слабке місце у захисті – сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії котрим у системі ТЗІ відсутні.

Вилом у захисті – сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії котрим у системі ТЗІ присутні, але перебувають у непрацюючому стані.

Неформальний опис – опис на звичайній мові, що не підлягає будь-яким обмеженням, за винятком необхідності використання звичайних умовностей граматики та синтаксису мови, яка використовується (при цьому багатозначність щодо трактування опису не виключається).

Напівформальна специфікація – специфікація, яка потребує використання обмежувальних позначень (наприклад, діаграм структур даних або процесів, мови специфікацій SDL і т. ін.) при додержанні певних умовностей, котрі мають неформальний опис (при цьому багатозначність щодо трактування опису повністю не виключається).

Формальна специфікація – специфікація, яка потребує використання лише формальної системи правил та позначень, побудованої на обгрунтованій математичній концепції (при цьому ймовірність багатозначності щодо трактування специфікації визначається ступенем обгрунтованості математичної концепції, що використовується).

Тест на проникнення – опис (специфікація) процедури штатних дій санкціонованого користувача або експерта, що імітує дії потенційного порушника з метою перевірки ефективності системи захисту ("глибина" тесту на проникнення визначається ступенем наближення дій, що імітуються, до реально можливих дій та ресурсними можливостями порушника).

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 оцінюваних робіт.

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

Оцінка АТС за критеріями ТЗІ – комплекс спеціалізованих дослідно-аналітичних і 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 на 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 реалізації системи ТЗІ на АТС.

Довірчі критерії – нормуючи 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.*

Специфікація ФПЗ (рівня стійкості механізму захисту) на АТС – опис технічних вимог, показників функціонування, нормуючих та обмежуючих умов, яких слід дотримуватися в процесі реалізації цієї ФПЗ (цього механізма захисту), якщо оцінка рівня захищеності інформаційних ресурсів АТС виконується або буде виконуватися відповідно до вимог НД ТЗІ 2.3-001-99.

ПРД - правила розподілу доступу.

ОЗП - оперативно-запам'ятовуючий пристрій.

4 Загальні положення

4.1 Цей документ містить у собі:

– множину специфікованих ФПЗ, якими слід користуватися в процесі створення моделі захисту інформаційних ресурсів АТС, якщо оцінка рівня захищеності цих ресурсів виконується або буде виконуватися відповідно до вимог НД ТЗІ 2.3-001-99;

– специфікації ФПЗ для АТС, які слід використовувати, якщо оцінка рівня захищеності інформаційних ресурсів АТС виконується або буде виконуватися відповідно до вимог НД ТЗІ 2.3-001-99;

– специфікації рівнів стійкості механізмів захисту, які реалізують специфіковані у цьому документі ФПЗ. В процесі створення моделі захисту інформаційних ресурсів АТС (див. НД ТЗІ 2.7-001-99) припустимо використання ФПЗ та відповідних механізмів захисту, специфікації котрих не знайшли відображення в цьому документі. Специфікації таких ФПЗ та механізмів захисту мають бути узгоджені з уповноваженим державним органом з питань ТЗІ.

– ФПЗ в цьому документі специфіковані відносно таких п'яти видів загроз (див. НД ТЗІ 1.1-001-99):

– порушення конфіденційності (тобто, ознайомлення з інформацією неавторизованними особами);

– порушення цілісності (тобто, несанкціонована законним власником зміна, підміна або знищення інформації);

– порушення доступності або відмова в обслуговуванні (тобто, позаштатні обмеження в реалізації авторизованими користувачами штатних процедур доступу до інформаційних ресурсів, зокрема через збої або відмови в роботі устаткування або програмних засобів);

– порушення спостережності або керованості (тобто, порушення штатних процедур ідентифікації і(або) автентифікації, контролю за доступом і контролю дій користувачів, повна або часткова втрата керованості станцією);

– несанкціоноване користування інформаційними ресурсами станції (у т.ч., несанкціоноване користування послугами, наданими станцією і т. ін.).

4.2 Специфікації ФПЗ структуровані також щодо відомих видів технічних каналів витоків інформації, каналів спеціальних впливів на інформаційні ресурси АТС та каналів НСД (див. НД ТЗІ 1.1-001-99).

5 Специфікації ФПЗ

5.1 Система ТЗІ на АТС у відповідності до НД ТЗІ 1.1-001-99 та НД ТЗІ 2.3-001-99 повинна надавати певну номенклатуру ФПЗ.

Для оцінки коректності (слушності) проекту КЗМЗ на АТС відповідно до НД ТЗІ 2.7-001-99 необхідно переконатися, що всі ФПЗ, які включені в модель захисту інформаційних ресурсів АТС, повною мірою і безпомилково реалізуються в техно-робочому проекті системи ТЗІ згідно з нормованими специфікаціями цих послуг.

Специфікації можливих на АТС ФПЗ з позначенням видів загроз (див. п. 5.3), яким ці ФПЗ запобігають, наведені у таблиці 6.

5.2 У цьому документі прийняте позначення можливих ФПЗ для АТС за допомогою термів довільної довжини.

Для позначення ФПЗ використовуються наведені нижче синтаксичні і семантичні правила формування термів – позначень ФПЗ.

Перший символ терма – літера Ф, дозволяє відрізнити позначення (терм) ФПЗ АТС від інших термів.

Другий і третій символи терма – двозначне десяткове число (код підсистеми), що відображає тип підсистем захисту інформаційних ресурсів АТС, які структуровані за видами технічних каналів витоку, спеціальних впливів та НСД (див. НД ТЗІ 1.1-001-99). Перелік та кодування типів підсистем захисту інформаційних ресурсів АТС наведено у таблиці 1.

Таблиця 1 Кодування підсистем захисту інформаційних ресурсів на АТС

Код підсистеми	Тип підсистеми захисту інформаційних ресурсів АТС
01	Підсистема захисту від несанкціонованих впливів суб'єктів доступу через штатні термінали обслуговування і штатні абонентські прикінцеві пристрої
02	Підсистема захисту від позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби АТС (але не через штатні засоби доступу)
03	Підсистема захисту від позаштатних впливів на параметри середовища експлуатації АТС
04	Підсистема захисту від впливів позаштатними технічними і (або) програмно-технічними засобами на елементи устаткування в процесі експлуатації АТС
05	Підсистема захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені під час її експлуатації
06	Підсистема захисту від впливів закладних пристроїв і програмних закладок
07	Підсистема захисту від витоків інформації через канали побічних електромагнітних випромінювань та наводів (ПЕМВН)
08	Підсистема захисту від витоків інформації через канали побічних акусто-електричних перетворень
09	Підсистема захисту від якісної недостатності інформаційно уразливих режимів, функцій і послуг, що надаються АТС
10	Підсистема захисту від збоїв та відмов у роботі АТС
11	Підсистема захисту від загроз у системах збереження інформації на фізичних носіях

Крім того, за допомогою другого та третього символів терму кодуються, поряд з вищенаведеними типами підсистем захисту, ще й інші види забезпечення систем ТЗІ на АТС (див. розділ 10 НД ТЗІ 1.1-001-99) таким чином:

– система ліквідації наслідків реалізованих загроз для інформації на АТС – десяткове число "12";

– система керування засобами ТЗІ – десяткове число "13".

Специфікації функцій системи організаційно-технічних заходів щодо захисту інформаційних ресурсів АТС (протидія загрозам, що не охоплені технічними засобами та механізмами захисту, протидія "слабким місцям" та "виломам" у захисті, здійснення гарантій захисту і т. ін.) наведені в НД ТЗІ 2.5-002-99 та НД ТЗІ 2.5-003-99.

Решта символів терма є послідовність змістовних скорочень, що поєднані між собою спеціальними розмежувачами, які разом із трьома попередніми символами утворюють у контексті код ФПЗ.

Змістовні скорочення складаються з трьох семантичних частин:

– скорочення для позначення дій (дієслова);
– скорочення для позначення місць і (або) предметів розгляду (іменники);
– скорочення для уточнення дій, місць та предметів розгляду (прикметники).

Дієслова мають трьохлітерні мнемонічні позначення. Іменники позначаються двома літерами. Позначення прикметників – однолітерні.

Повний перелік скорочень для позначень дій наведено у таблиці 2.

Таблиця 2 Скорочені позначення дій (дієслова)

Скорочення дієслова	Опис дії
АНЛ	аналіз
АУД	аудит
БЛК	блокування
ВИК	виключення, відключення
ВКР	використання
ВЯВ	виявлення, сигналізація і реєстрація
ЗМН	зменьшення
ЗНЩ	з контексту: – знищення; – знешкодження
ЗРЧ	підвищення зручностей користування
ІЗЛ	ізоляція
КЕР	керування
КТР	контроль, нагляд, спостереження, виявлення
МНЛ	використання методу нелінійної локації
МОН	моніторинг
МРК	маркування
МСК	маскування
НМР	надмірність (не резервування)
НОВ	відновлення
НТР	нейтралізація (спроб НСД, впливу, відхилень параметрів і т. ін.)
ОРГ	організаційні заходи
ОСЛ	ослаблення, екранізація
ОХР	охорона
ПВІ	безпосередня протидія витоку інформації
ПДТ	пристосованість до транспортування
ПТД	протидія
ПТР	підтримка
РЕС	реєстрація
РДЛ	розподіл, рознесення
РДО	розмежування доступу
РЕЗ	резервування

Скорочення дієслова	Опис дії
РКФ	реконфігурація
СКР	скремблювання
ТСТ	тестування
ШФР	шифрування

Для позначення місця і (або) предмету розгляду застосовуються скорочення, які наведені у таблиці 3.

Таблиця 3 Позначення місць та предметів розгляду (іменники)

Скорочення	Місце і (або) предмет розгляду
АВ	аудиторська вибірка
АЕ	акусто-електричні перетворення та їх (інформативні) сигнали
АЛ	з контексту: – абонентська лінія, абонентський канал; – абонент; – телефонний комутатор; – прикінцевий абонентський пристрій
АН	засоби аналізу
ВМ	випромінювання
ВС	відмовостійкість
ВЧ	сигнали «ВЧ-накачки»
ДЗ	тестове та діагностичне забезпечення
ЕЗ	запасні елементи (устаткування)
ЕЛ	електричні параметри
ЕМ	електромагнітне випромінювання
ЕП	енергопостачання
ЕУ	елементи устаткування
ЗБ	з контексту: – збій; – відмова; – помилка
ЗВ	з контексту: – позаштатні засоби впливу; – атакуючі засоби
ЗЄ	з’єднання
ЗЗ	з контексту: – засіб захисту; – система захисту; – база захисту
ЗК	закладні пристрої
ЗМ	засоби модіфікації
ЗН	засоби нейтралізації
ЗП	запасні елементи
ЗР	засоби розробки та відлагодження
ЗС	засоби спостереження
ЗХ	з контексту: – захищена зона, включаючи межі захищеної зони; – захист

Скорочення	Місце і (або) предмет розгляду
ІС	ініціюючі сигнали (наприклад, закладних пристроїв)
ІУ	інформаційно уразливі режими, функції та послуги
КВ	канали витоку
КФ	конфігурація
ЛК	лінії комунікацій
ЛУ	лінії ущільнення абонентських каналів
МА	моменти активізації
МВ	місце відмови
МЗ	межа зони, що захищається (а не всієї захищеної зони)
МЛ	міжстанційні лінії зв'язку та лінії міжстанційної сигналізації і синхронізації
МО	монітори обслуговування
НВ	процес відновлення
НД	навід
НК	несанкціоноване користування
НМ	потенційно небезпечне місце
НП	негативні впливи
ОД	об'єкт доступу
ОП	область пам'яті, оперативна пам'ять, основна пам'ять
ПД	порушення доступності
ПЕ	побічне електромагнітне випромінювання
ПЗ	програмний засіб, програмне забезпечення
ПК	підсистема комутації абонентських і з'єднувальних ліній зв'язку (КАЗЛ) на АТС
ПР	протокол
ПС	послуга
ПЦ	з контексту: – процес; – процедура
РЕ	зона розміщення елементів АТС
РР	ресурс
СГ	сигнал
СД	суб'єкт доступу
СЗ	системні засоби
СК	підсистема керування на АТС
СЩ	з контексту: – середовище (наприклад, навколишнє); – параметри контрольованих частин устаткування
ТВ	час відновлення
ТЗ	технічні (апаратні) засоби, технічне (апаратне) забезпечення
ТЛ	з контексту: – термінальні лінії; – термінал
ТО	технічне обслуговування
ТР	температура
УО	уповноважена особа (адміністратор захисту)
УФ	ультрафіолетове випромінювання
ФЕ	елементи однакового функціонального призначення, але різні за фізичною природою.

Скорочення	Місце і (або) предмет розгляду
ФН	фізичні носії
ЦЛ	автентичність (цілісність)
ЧВ	режим чекання виклику
ШС	прошарки технологічного середовища

Для уточнення дії, місця і (або) предмету розгляду використовуються скорочення, що наведені у таблиці 4.

Таблиця 4 Позначення уточнюючих прикметників для місць та предметів розгляду

Скорочення	Уточнюючий прикметник
А	з контексту: – аналоговий (наприклад, АЛ/А); – алгоритмічний (наприклад, ПЗ/А, М/А)
Б	безперервний
Г	груповий, спільний
Д	з контексту: – доказовий (наприклад, метод програмування); – довірчий, дискреційний
Е	помилковий
З	запасні
І	з контексту: – інформаційний; – інформативний (наприклад, про канали витоку)
М	з контексту: – апаратний (схемотехнічний, «виготовлений з мікросхем»); – механічний; – модульний
Н	мандатний
О	індивідуальний, поодинокий
П	з контексту: – повний (наприклад, про тестування); – загальний; – просторовий
С	структурний
Т	з контексту: – періодичний; – той, що відбувається у часі
Ф	функціональний
Ц	цифровий
Ш	штатний
Щ	позаштатний, несанкціонований

При позначенні, якщо це необхідно, вказується кілька місць або предметів розгляду, що розмежовуються між собою позначками, семантика котрих розшифровується у таблиці 5.

Таблиця 5 Семантика розмежувачів

Позначка	Семантика
/	– завдяки (комусь, чомусь); – через (когось, щось); – за поміччю (когось, чогось); – за допомогою (когось, чогось); – одночасно з …; – ким або чим виконується дія (наприклад, який, що перевіряє)
\	– приймається до; – призначається до; – для (чогось, когось); – над ким (чим) виконується дія (наприклад, чим перевіряється, що контролюється)
’	і (або)

Частина позначення …/РДО/ТЗ вказує, що маються на увазі правила розмежування доступу, що реалізовані через технічні засоби (або, інакше кажучи, за допомогою технічних засобів).

Частина позначення …/РДО\ТЗ вказує, що маються на увазі правила розмежування доступу (застосовані) до технічних засобів (елементів устаткування).

Частина позначення …/ТЗ’ПЗ\ПС\УО вказує, що мається на увазі технічне і (або) програмне забезпечення для підтримки послуг адміністраторів захисту (уповноважених осіб).

Запис частини специфікації послуги змінної довжини завжди починається із розмежувача «/» і має ієрархічну структуру: скорочення, що розміщене у запису специфікації лівіше, має більш загальний зміст ніж скорочення, що міститься правіше.

Приклад 1. Ф01/РДО/Д/АЛ\ПС – мнемонічне позначення ФПЗ, що протидіє загрозам спеціальних впливів суб’єктів доступу через штатні термінали обслуговування і штатні абонентські прикінцеві пристрої (01). Конкретний зміст цієї ФПЗ специфікується за допомогою підтерма /РДО/Д/АЛ\ПС – розмежування доступу (РДО) з використанням довірчих (Д) правил з боку телефонних комутаторів і прикінцевих абонентських пристроїв (АЛ), які застосовуються до сервісних функцій і послуг (ПС) АТС (див. таблицю 6).

Кожній ФПЗ ставиться у відповідність перелік загроз, яким вона запобігає. Види загроз закодовані однією літерою слов’янського алфавіту, а саме:

К – порушення конфіденційності;

Ц – порушення цілісності;

Д – порушення доступності;

С – порушення спостережності або керованості;

Р – несанкціоноване користування ресурсами.

Приклад 2. Для ФПЗ Ф01/РДО/Д/АЛ\ПС, що наведена у прикладі 1, перелік загроз КЦ__Р складається з усіх перелічених вище загроз, за винятком порушень доступності і порушень спостержності або керованості.

Таблиця 6 Специфікації ФПЗ

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
1 Підсистема захисту від несанкціонованих впливів суб'єктів доступу через штатні термінали обслуговування і штатні абонентські прикінцеві пристрої		
Ф01/РДО/Д/МО\ПЦ\СК	Розмежування доступу за допомогою довірчих (дискреційних) правил для суб'єктів та їх процесів з боку моніторів обслуговування до програм, даних, процесів і пристроїв у підсистемі керування АТС	КЦДСР
Ф01/РДО/Д/АЛ\ПС	Розмежування доступу за допомогою довірчих (дискреційних) правил з боку телефонних комутаторів і прикінцевих абонентских пристроїв, які застосовуються до сервісних функцій і послуг АТС	КЦ__Р
Ф01/РДО/Н/МО\ПЦ\СК	Розмежування доступу за допомогою мандатних правил для суб'єктів та їх процесів з боку моніторів обслуговування, які застосовуються до програм, даних, процесів і пристроїв в підсистемі керування АТС	КЦДСР
Ф01/РДО/Н/АЛ\ПС	Розмежування доступу за допомогою мандатних правил, що застосовуються з боку телефонних комутаторів і прикінцевих абонентських пристроїв до сервісних функцій і послуг АТС	КЦ__Р
Ф01/РДО/Д'Н/МО\ПЦ\СК	Використання змішаної стратегії керування доступом, що застосовується з боку моніторів обслуговування до програм, даних, процесів та пристроїв підсистеми керування АТС	КЦДСР
Ф01/РДО/Д'Н/АЛ\ПС	Використання змішаної стратегії керування доступом, що застосовується з боку телефонних комутаторів і прикінцевих абонентських пристроїв до сервісних функцій і послуг АТС	КЦ__Р
Ф01/МРК\Н\РР\І	Маркування інформаційних ресурсів АТС у випадках використання мандатних правил	КЦ__Р
Ф01/МРК\Д'Н\РР\І	Маркування інформаційних ресурсів АТС у разі використання змішаних правил	КЦ__Р
Ф01/ІЗЛ\ЗЗ	Ізоляція засобів бази захисту АТС	КЦ___
Ф01/ІЗЛ\СЗ	Ізоляція системних засобів АТС	КЦ___
Ф01/ІЗЛ\РР\Г	Ізоляція базових засобів АТС, тобто станційних ресурсів спільного користування	КЦ___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф01/ІЗЛ\ОП\СД	Ізоляція областей пам'яті, відведених суб'єктам доступу	КЦ___
Ф01/ЗНЩ\ОП\ОД	Очищення областей пам'яті об'єктів перед їхнім повторним використанням	К____
Ф01/РДО\ОД\СД	Розподіл об'єктів доступу між суб'єктами АТС	КЦ__Р
Ф01/ШФР\РР\І\СК	Шифрування інформації в підсистемі керування АТС	КЦ___
Ф01/ШФР\РР\І\АЛ	Шифрування інформації в підсистемі комутації абонентських каналів зв'язку	КЦ___
Ф01/СКР\РР\І\АЛ	Скремблювання інформації в підсистемі комутації абонентських каналів зв'язку на АТС	КЦ___
Ф01/БЛК\ОД	Блокування об'єктів доступу при спробі НСД	КЦ__Р
Ф01/НМР/РР/І	Введення інформаційної надмірності ресурсів АТС (наприклад, надлишкове кодування)	_Ц___
Ф01/НМР/РР/М	Введення апаратної надмірності елементів і (або) підсистем АТС	_Ц___
Ф01/ВИК\ЗР'ЗМ\ПЗ\Ш	Виключення з операційного середовища АТС засобів розробки та відлагодження програм, а також засобів спостереження та модифікації об'єктного коду програм	КЦД__
Ф01/ТСТ/Т\ЦЛ\КФ\ПЗ'ТЗ	Періодичні перевірки цілісності конфігурації програмно-технічних засобів АТС	КЦДСР
Ф01/ТСТ/Т\ЦЛ\ЗЗ	Періодичні перевірки цілісності засобів бази захисту АТС, включаючи контроль цілісності системи розмежування доступу (СРД)	КЦДСР
Ф01/ТСТ/Т\ЦЛ\ДЗ	Періодичні перевірки цілісності тестового і діагностичного забезпечення АТС	_Ц___
Ф01/ЗНЩ\ОД	Знищення (стирання) об'єктів доступу у разі спроби НСД	К____
Ф01/ПТД\ЗЄ\Е	Використання механізмів запобігання помилкових з'єднань на станції	К____
Ф01/ПТД\ПС\Е	Використання механізмів запобігання помилкового надання сервісних послуг станцією (як абонентам станції, так і обслуговуючому персоналу)	К____
Ф01/ПТР/ПС\УО	Технічна підтримка послуг для спеціально уповноважених осіб (наприклад, адміністратора захисту)	КЦ___
Ф01/АНЛ/ПР\СК	Аналіз лістингів протоколів ідентифікації й автентифікації (перевірки істинності) користувачів підсистеми керування АТС	___С_

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф01/АНЛ/ПР\АЛ	Аналіз протоколів ідентифікації й автентифікації абонентів АТС	___С_
Ф01/АУД\СК	Аудит (контролю дій суб'єктів) у підсистемі керування АТС	___С_
Ф01/АУД\АЛ	Аудит (контролю дій абонентів) у підсистемі комутації абонентських каналів зв'язку АТС	___С_
Ф01/КТР\ШС	Індикація прошарків технологічного середовища АТС	___С_
Ф01/ТСТ\ЦЛ\ПЗ'ТЗ	Спостереження за процесами, пов'язаними з перевіркою автентичності (цілісності) програмно-технічних засобів АТС, включаючи перевірки на коректність виконуваних на АТС операцій	___С_
Ф01/ПТР/ПЗ/АН\АВ	Підтримка програмних засобів аналізу аудиторських вибірок	___С_
Ф01/ПТР/ПЗ\ЗЗ	Підтримка засобів спостереження за процедурами тестування бази захисту АТС у процесі її експлуатації	___С_
Ф01/ВЯВ/ТЛ\НК	Виявлення, сигналізація і реєстрація спроб НСД (на термінал адміністратора і порушника)	___С_
2 Підсистема захисту від позаштатних впливів через штатні основні або штатні додаткові програмні і (або) технічні засоби АТС (але не через штатні засоби доступу)		
Ф02/ШФР\РР\І\СК	Шифрування інформації в підсистемі керування АТС	КЦ___
Ф02/ШФР\РР\І\АЛ	Шифрування інформації в підсистемі комутації абонентських каналів зв'язку	КЦ___
Ф02/СКР\РР\І\АЛ	Скремблювання інформації в підсистемі комутації абонентських каналів зв'язку	К____
Ф02/БЛК\ОД\ЗВ	Блокування об'єкта доступу в разі виявлення позаштатних впливів	КЦ___
Ф02/ЗНЩ\ОД\ЗВ	Знищення (стирання) об'єктів доступу в разі виявлення позаштатних впливів	К____
Ф02/ІЗЛ\ЗВ/ПЗ'ТЗ/Ш	Ізоляція об'єктів позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби	КЦ___
Ф02/РДО/ПЦ/ПЗ'ТЗ/Ш\НМ	Розмежування доступу до процесів, що ініціюються з боку потенційно небезпечних місць, з яких можливий позаштатний вплив через штатні програмні і (або) технічні засоби	КЦ___
Ф02/ТСТ\ЦЛ\ЗЗ\ЗВ/Ш	Перевірка цілісності засобів захисту від позаштатних впливів через штатні засоби АТС	_Ц___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф02/ВЯВ\ЗВ/ПЗ’ТЗ/Ш	Виявлення, сигналізація і реєстрація спроб позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби	___С_
Ф02/ТСТ/ЗС\ЗЗ\ЗВ	Застосування засобів спостереження за процедурами тестування і діагностування технічних і програмних засобів захисту від позаштатних впливів	___С_
Ф02/ТСТ\ЗЗ\ЗВ	Застосування засобів тестування системи захисту від позаштатних впливів	___С_
Ф02/МОН\ЗВ\ПЗ’ТЗ\Ш	Підтримка засобів моніторингу програмно-технічних засобів АТС на предмет виявлення позаштатних впливів через штатні засоби	___С_
Ф02/ВЯВ/О\НК\АЛ\А	Застосування індивідуальних засобів виявлення несанкціонованого користування аналоговою абонентською лінією АТС	____Р
Ф02/ВЯВ/О\НК\АЛ\Ц\Ш	Застосування індивідуальних засобів виявлення несанкціонованого користування цифровою абонентською лінією АТС за допомогою штатного цифрового абонентського прикінцевого пристрою	____Р
Ф02/ПТД/Г/ТЗ\НК\АЛ\А\Ш	Застосування групових засобів протидії з боку станційного устаткування несанкціонованому користуванню штатними аналоговими абонентськими прикінцевими пристроями	____Р
Ф02/ПТД/Г/ТЗ\НК\АЛ\Ц\Ш	Застосування групових засобів протидії з боку станційного устаткування несанкціонованому користуванню штатними цифровими абонентськими прикінцевими пристроями	____Р
Ф02/ПТД/О\НК\АЛ	Застосування індивідуальних засобів протидії несанкціонованому користуванню абонентською лінією	____Р
3 Підсистема захисту від позаштатних впливів на параметри середовища експлуатації АТС		
Ф03/ПТР\ТР	Підтримка оптимальної температури навколишнього середовища АТС	__Д__
Ф03/ВЯВ\ЕП	Виявлення і реєстрація відхилень параметрів енергопостачання АТС	__Д__
Ф03/НТР\ЕП	Нейтралізація змін параметрів енергопостачання АТС	__Д__
Ф03/ВЯВ\ЕМ	Виявлення і реєстрація підвищення фону електромагнітних випромінювань (ЕМВ) у приміщеннях АТС	__Д__
Ф03/НТР\ЕМ	Нейтралізація впливів ЕМВ	__Д__

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф03/ВЯВ\УФ	Виявлення і реєстрація ультрафіолетового випромінювання (УФВ)	__Д__
Ф03/НТР\УФ	Нейтралізація впливу УФВ	__Д__
Ф03/ПВІ/ЗЗ\НМ\ЕУ	Захист ліній зв'язку шляхом застосування захисних пристроїв у критичних елементах устаткування	__Д__
Ф03/ОХР/ТЗ	Наявність спеціальних упаковок, віброгасників, захисних покриттів під час транспортування та зберігання	__Д__
Ф03/НТР\ЗВ\СЩ\ПЗ'ТЗ	Наявність засобів активної нейтралізації джерел негативних впливів на програмно-технічні засоби АТС, що виходять із зовнішнього середовища функціонування АТС	__Д__
4 Підсистема захисту від впливів позаштатними технічними і (або) програмно-технічними засобами на елементи устаткування в процесі експлуатації АТС		
Ф04/ШФР\РР\І\СК	Шифрування інформації в підсистемі керування АТС	КЦ___
Ф04/ШФР\РР\І\АЛ	Шифрування інформації в підсистемі комутації абонентських каналів зв'язку	КЦ___
Ф04/СКР\РР\І\АЛ	Скремблювання інформації в підсистемі комутації абонентських каналів зв'язку	К____
Ф04/БЛК\ОД\ЗВ\ЕУ	Блокування об'єктів доступу у випадку виявлення впливів позаштатними засобами на елементи устаткування АТС	КЦ___
Ф04/ЗНЩ\ОД\ЗВ\ЕУ	Знищення (стирання) об'єктів доступу у випадку виявлення впливів позаштатними засобами на елементи устаткування АТС	К____
Ф04/ІЗЛ\ОД\ЗВ\ЕУ	Ізоляція об'єктів доступу у випадку виявлення впливів позаштатними засобами на елементи устаткування АТС	КЦ___
Ф04/МСК\ОД\ЗВ\ЕУ	Маскування (зашумлення) об'єктів доступу у випадку виявлення впливів позаштатними засобами на елементи устаткування АТС	К____
Ф04/РДО\ПЦ\ЗВ\ЕУ	Розмежування доступу до процесів, що ініціюються з боку позаштатних засобів впливів на елементи устаткування АТС	КЦ___
Ф04/ЗНЩ\ЗВ	Знищення (знешкодження) засобів, що атакують	КЦ___
Ф04/ТСТ\ЦЛ\ЗЗ\ЗВ\ЕУ	Контроль цілісності засобів захисту від впливів позаштатними засобами на елементи устаткування АТС	_Ц___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф04/ВЯВ\ЗВ/ПЗ’ТЗ\ЕУ	Виявлення, сигналізація і реєстрація спроб впливів позаштатними технічними і (або) програмно-технічними засобами на елементи устаткування в процесі експлуатації АТС	___С_
Ф04/ТСТ\ЗЗ\ЗВ\ЕУ	Наявність засобів тестування і засобів спостереження за процесами, пов’язаними з перевіркою коректності системи захисту від впливів позаштатними засобами на елементи устаткування в процесі її експлуатації	___С_
Ф04/КЕР\ЗН\ЗВ\ЕУ	Керування засобами нейтралізації позаштатних впливів на елементи устаткування АТС	___С_
Ф04/МОН\ПЗ’ТЗ\ЗВ\ЕУ	Наявність засобів моніторингу програмно-технічних засобів АТС на предмет виявлення впливів позаштатними засобами на елементи устаткування АТС	___С_
Ф04/ВЯВ/ПЗ’ТЗ/О\НК\АЛ\А	Застосування індивідуальних засобів для виявлення несанкціонованого користування аналоговою абонентською лінією АТС за допомогою нештатних технічних і (або) програмно-технічних засобів	____Р
Ф04/ПТД/ТЗ/О\НК\АЛ\А	Застосування індивідуальних засобів протидії несанкціонованому користуванню аналоговою абонентською лінією АТС	____Р
Ф04/ПТД/ТЗ/О\НК\АЛ\Ц	Застосування індивідуальних засобів протидії несанкціонованому користуванню цифровою абонентською лінією АТС	____Р
Ф04/ПТД/Г/ЕУ\НК\АЛ\А	Застосування групових засобів протидії з боку станційного устаткування несанкціонованому користуванню аналоговими абонентськими лініями	____Р
Ф04/ПТД/Г/ЕУ\НК\АЛ\Ц	Застосування групових засобів протидії з боку станційного устаткування несанкціонованому користуванню цифровими абонентськими лініями	____Р
5 Підсистема захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені під час її експлуатації		
Ф05/ШФР\РР\І\СК	Шифрування інформації в підсистемі керування АТС	КЦ___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф05/ШФР\РР\І\АЛ	Шифрування інформації в підсистемі комутації абонентських каналів зв'язку	КЦ___
Ф05/СКР\РР\І\АЛ	Скремблювання інформації в підсистемі комутації абонентських каналів зв'язку	К____
Ф05/БЛК\ОД\ЗВ\ПЦ	Блокування об'єкта доступу у випадку виявлення впливів позаштатними засобами на програми, дані і процеси на АТС	КЦ___
Ф05/ЗНЩ\ОД\ЗВ\ПЦ	Знищення (стирання) об'єктів доступу у випадку виявлення впливів позаштатними засобами на програми, дані і процеси на АТС	К____
Ф05/ІЗЛ\ОД\ЗВ\ПЦ	Ізоляція об'єктів доступу у випадку виявлення впливів позаштатними засобами на програми, дані і процеси на АТС	КЦ___
Ф05/МСК\ОД\ЗВ\ПЦ	Маскування об'єктів доступу у випадку виявлення впливів позаштатними засобами на програми, дані і процеси на АТС	К____
Ф05/РДО\ПЦ\ЗВ	Розмежування доступу до процесів, що ініціюються з боку позаштатних засобів впливів на програми, дані і процеси на АТС	КЦ___
Ф05/ЗНЩ\ЗВ	Знищення (знешкодження) атакуючих засобів	КЦ___
Ф05/КТР\ЦЛ\ЗЗ\ЗВ\ПЦ	Перевірка цілісності засобів захисту від впливів позаштатними засобами на програми, дані і процеси на АТС	_Ц___
Ф05/ВЯВ\ЗВ/ПЗ'ТЗ\ПЦ	Виявлення, сигналізація і реєстрація спроб впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС	___С_
Ф05/ТСТ\ЗЗ\ЗВ\ПЦ	Наявність засобів тестування і спостереження за процесами, пов'язаними з перевіркою коректності системи захисту від впливів позаштатними засобами на програми, дані і процеси на АТС	___С_
Ф05/МОН\ПЗ'ТЗ\ЗВ\ПЦ	Наявність засобів моніторингу програмно-технічних засобів АТС на предмет виявлення позаштатних впливів на програми, дані і процеси на АТС	___С_
Ф05/КЕР\ЗЗ'ЗН\ЗВ\ПЦ	Керування засобами захисту та нейтралізації позаштатних впливів на програми, дані і процеси на АТС	___С_
Ф05/ІЗЛ\СЗ/ПЗ	Ізоляція модулів системного програмного забезпечення	____Р
Ф05/КТР\КФ'ЦЛ\ПЗ'ТЗ	Контроль конфігурації і цілісності програмно-технічних засобів АТС	____Р

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
6 Підсистема захисту від впливів закладних пристроїв і програмних закладок		
Ф06/ШФР\РР\І\СК	Шифрування інформації в підсистемі керування АТС	КЦ___
Ф06/ШФР\РР\І\АЛ	Шифрування інформації в підсистемі комутації абонентських каналів зв'язку	КЦ___
Ф06/БЛК\ОД\ЗК	Блокування об'єкта доступу у випадку виявлення закладних пристроїв	КЦ___
Ф06/ЗНЩ\ОД\ЗК	Знищення (стирання) об'єкта доступу у випадку виявлення закладних пристроїв	К____
Ф06/ІЗЛ\ОД\ЗК	Ізоляція об'єкта доступу випадку виявлення закладних пристроїв	КЦ___
Ф06/МСК\ОД\ЗК	Маскування об'єкта доступу у випадку виявлення закладних пристроїв	К____
Ф06/РДО\ПЦ/ЗК	Розмежування доступу до процесів, що ініціюються закладними пристроями	КЦ___
Ф06/ЗНЩ\ЗК'СГ	Знищення (знешкодження, нейтралізація) виявлених закладних пристроїв і (або) активізуючих їх сигналів	КЦ___
Ф06/КТР\ЦЛ\ЗЗ\ЗК/ПЗ'ТЗ	Контроль цілісності засобів захисту від програмних і (або) технічних закладних пристроїв	_Ц___
Ф06/МНЛ\ЗК	Виявлення закладних пристроїв методом нелінійної локації	___С_
Ф06/КТР\ЕЛ\ЗК\ЕУ	Виявлення закладних пристроїв методом реєстрації змін електричних параметрів контрольованих частин устаткування АТС	___С_
Ф06/КТР\КФ/ПЗ'ТЗ\ЗК	Виявлення закладних пристроїв за допомогою контролю конфігурації програмно-технічних засобів АТС	___С_
Ф06/ВЯВ\ЗК/ІС	Виявлення, сигналізація і реєстрація спроб активізації закладних пристроїв (що ініціюють сигнали і т. ін.)	___С_
Ф06/ВЯВ\ЗК/МА	Виявлення, сигналізація і реєстрація моментів активізації закладних пристроїв	___С_
Ф06/ТСТ/ЗС\ЗЗ\ЗК	Наявність засобів тестування і засобів спостереження за процесами, пов'язаними з перевіркою коректності системи захисту від закладних пристроїв	___С_
Ф06/МОН\ПЗ'ТЗ\ЗК/ІС	Наявність засобів моніторингу програмно-технічних засобів АТС на предмет виявлення закладних пристроїв, а також сигналів, що ініціюють їхню активізацію	___С_

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф06/ПТР/ЗН\ЗК	Підтримка засобів керування засобами нейтралізації закладних пристроїв	___С_
Ф06/ІЗЛ\СЗ/ПЗ	Ізоляція модулів системного програмного забезпечення	____Р
Ф06/КТР\КФ'ЦЛ\ПЗ'ТЗ	Контроль конфігурації і цілісності програмно-технічних засобів АТС	____Р
7 Підсистема захисту від витоків інформації через канали ПЕМВН		
Ф07/ВЯВ\ПЕ\МЗ	Виявлення (і сигналізація) побічного електромагнітного випромінювання в межах зон АТС, що захищаються	К____
Ф07/ВЯВ\ПЕ/І\МЗ	Виявлення (і сигналізація) інформативних складових побічних електромагнітних випромінювань в межах зон АТС, що захищаються	К____
Ф07/РЕС\ПЕ\МЗ	Реєстрація побічного електромагнітного випромінювання в межах зон АТС, що захищаються	К____
Ф07/РЕС\ПЕ/І\МЗ	Реєстрація інформативних складових побічних електромагнітних випромінювань в межах зон АТС, що захищаються	К____
Ф07/МОН\ПЕ\МЗ	Моніторинг побічного електромагнітного випромінювання в межах зон АТС, що захищаються	К____
Ф07/МОН\ПЕ/І\МЗ	Моніторинг інформативних складових побічних електромагнітних випромінювань в межах зон АТС, що захищаються	К____
Ф07/ОСЛ\ПЕ\МЗ	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) побічного електромагнітного випромінювання в межах зон АТС, що захищаються	К____
Ф07/ОСЛ\ПЕ\І\МЗ	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) інформативних складових побічних електромагнітних випромінювань в межах зон АТС, що захищаються	К____
Ф07/МСК\ПЕ\МЗ	Маскування (у т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) побічного електромагнітного випромінювання в межах зон АТС, що захищаються	К____

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф07/МСК\ПЕ/І\МЗ	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) інформативних складових побічних електромагнітних випромінювань в межах зон АТС, що захищаються	К____
Ф07/ВЯВ\НД/АЛ/Ц	Виявлення і сигналізація при виявленні наводів в цифрових абонентських лініях	К____
Ф07/ВЯВ\НД/АЛ/А	Виявлення і сигналізація при виявленні наводів в аналогових абонентських лініях	К____
Ф07/ВЯВ\НД/І/ЕМ/СГ/АЛ/А	Виявлення і сигналізація інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в аналогових абонентських лініях	К____
Ф07/РЕС\НД/АЛ/Ц	Реєстрація наводів в цифрових абонентських лініях	К____
Ф07/РЕС\НД/АЛ/А	Реєстрація наводів в аналогових абонентських лініях	К____
Ф07/РЕС\НД/І/ЕМ/СГ/АЛ/А	Реєстрація інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в аналогових абонентських лініях	К____
Ф07/ВЯВ\НД/І/ЕМ/СГ/АЛ/Ц	Виявлення і сигналізація інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в цифрових абонентських лініях	К____
Ф07/РЕС\НД/І/ЕМ/СГ/АЛ/Ц	Реєстрація інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в цифрових абонентських лініях	К____
Ф07/МОН\НД/АЛ/Ц	Моніторинг наводів в цифрових абонентських лініях	К____
Ф07/МОН\НД\АЛ/А	Моніторинг наводів в аналогових абонентських лініях	К____
Ф07/МОН\НД/І/ЕМ/СГ/АЛ/А	Моніторинг інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в аналогових абонентських лініях	К____
Ф07/МОН\НД/І/ЕМ/СГ/АЛ/Ц	Моніторинг інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в цифрових абонентських лініях	К____
Ф07/ОСЛ\НД/АЛ/Ц	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) наводів в цифрових абонентських лініях	К____

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф07/ОСЛ\НД/АЛ/А	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) наводів в аналогових абонентських лініях	К____
Ф07/ОСЛ\НД/І/ЕМ/СГ/АЛ/А	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів в аналогових абонентських лініях	К____
Ф07/ОСЛ\НД/І/ЕМ/СГ/АЛ/Ц	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в цифрових абонентських лініях	К____
Ф07/МСК\НД/АЛ/Ц	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) наводів в цифрових абонентських лініях	К____
Ф07/МСК\НД/АЛ/А	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) наводів в аналогових абонентських лініях	К____
Ф07/МСК\НД/І/ЕМ/СГ/АЛ/А	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в аналогових абонентських лініях	К____
Ф07/МСК\НД/І/ЕМ/СГ/АЛ/Ц	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) інформативних складових наводів від електромагнітних полів, які утворюються в процесі передачі сигналів, в цифрових абонентських лініях	К____
Ф07/ВЯВ\НД\ТЛ	Виявлення (і сигналізація) наводів в термінальних лініях (включаючи термінальні пристрої)	К____
Ф07/ВЯВ\НД\ЛУ	Виявлення (і сигналізація) наводів на лініях проміжного ущільнення абонентських каналів	К____
Ф07/ВЯВ\НД\МЛ	Виявлення і сигналізація у разі виявлення наводів в міжстанційних лініях зв’язку та лініях міжстанційної сигналізації і синхронізації	К____

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф07/ВЯВ\НД\ЛК\ЗХ	Виявлення і сигналізація у разі виявлення наводів в лініях комунікацій в межах і на межі зон, що захищаються	К____
Ф07/РЕС\НД\ТЛ	Реєстрація наводів в термінальних лініях (включаючи термінальні пристрої)	К____
Ф07/РЕС\НД\ЛУ	Реєстрація наводів в лініях проміжного ущільнення абонентських каналів	К____
Ф07/РЕС\НД\МЛ	Реєстрація наводів в міжстанційних лініях зв'язку та лініях міжстанційної сигналізації і синхронізації	К____
Ф07/РЕС\НД\ЛК\ЗХ	Реєстрація наводів в лініях комунікацій в межах і на межі зон, що захищаються	К____
Ф07/МОН\НД\ТЛ	Моніторинг наводів в термінальних лініях (включаючи термінальні пристрої)	К____
Ф07/МОН\НД\ЛУ	Моніторинг наводів в лініях проміжного ущільнення абонентських каналів	К____
Ф07/МОН\НД\МЛ	Моніторинг наводів в міжстанційних лініях зв'язку та лініях міжстанційної сигналізації і синхронізації	К____
Ф07/МОН\НД\ЛК\ЗХ	Моніторинг наводів в лініях комунікацій в межах і на межі зон, що захищаються	К____
Ф07/ОСЛ\НД\ТЛ	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) наводів в термінальних лініях (включаючи термінальні пристрої)	К____
Ф07/ОСЛ\НД\ЛУ	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) наводів в лініях проміжного ущільнення абонентських каналів	К____
Ф07/ОСЛ\НД\МЛ	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) наводів в міжстанційних лініях зв'язку та лініях міжстанційної сигналізації і синхронізації	К____
Ф07/ОСЛ\НД\ЛК\ЗХ	Ослаблення (у т.ч., за рахунок екранування, симетріювання, заземлення і т. ін.) наводів в лініях комунікацій в межах і на межі зон, що захищаються	К____
Ф07/МСК\НД\ТЛ	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) наводів в термінальних лініях (включаючи термінальні пристрої)	К____

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф07/МСК\НД\ЛУ	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) наводів в лініях проміжного ущільнення абонентських каналів	К____
Ф07/МСК\НД\МЛ	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) наводів в міжстанційних лініях зв'язку та лініях міжстанційної сигналізації і синхронізації	К____
Ф07/МСК\НД\ЛК\ЗХ	Маскування (в т.ч., за рахунок зашумлення, генерації маскуючих сигналів і т. ін.) наводів в лініях комунікацій в межах і на межі зон, що захищаються	К____
8 Підсистема захисту від витоків інформації через канали побічних акусто-електричних перетворень		
Ф08/ВЯВ\АЕ\АЛ\А	Виявлення (і сигналізація) сигналів побічних акусто-електричних перетворень на прикінцевих пристроях аналогових абонентських ліній	К____
Ф08/ВЯВ\АЕ\ТЛ\СК	Виявлення (і сигналізація) сигналів акусто-електричних перетворень на термі-нальних пристроях підсистеми керування станцією	К____
Ф08/ВЯВ\СГ/ВЧ\АЛ\Ц	Виявлення (і сигналізація) сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях цифрових абонентських ліній зв'язку	К____
Ф08/ВЯВ\СГ/ВЧ\АЛ\А	Виявлення (і сигналізація) сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях аналогових абонентських ліній зв'язку	К____
Ф08/ВЯВ\СГ/ВЧ\ТЛ\СК	Виявлення (і сигналізація) сигналів ВЧ-коливань («ВЧ-накачки») на термінальних пристроях підсистеми керування АТС	
Ф08/ВЯВ\ВМ/ВЧ\ЕМ	Виявлення (і сигналізація) випромінювання електромагнітних полів, що створюються в процесі генерації сигналів сторонніх ВЧ-коливань («ВЧ-накачки»)	К____
Ф08/РЕС\АЕ\АЛ\А	Реєстрація сигналів побічних акусто-електричних перетворень на прикінцевих пристроях аналогових абонентських ліній	К____
Ф08/РЕС\АЕ\ТЛ\СК	Реєстрація сигналів побічних акусто-електричних перетворень на термінальних пристроях підсистеми керування станцією	К____

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф08/РЕС\АЕ/І/Ц\АЛ\А	Реєстрація цифрових інформативних складових сигналів побічних акусто-електричних перетворень на прикінцевих пристроях аналогових абонентських ліній	К____
Ф08/РЕС\СГ/ВЧ\АЛ\Ц	Реєстрація сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях цифрових абонентських ліній зв'язку	К____
Ф08/РЕС\СГ/ВЧ\АЛ\А	Реєстрація сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях аналогових абонентських ліній зв'язку	К____
Ф08/РЕС\СГ/ВЧ\ТЛ\СК	Реєстрація сигналів ВЧ-коливань («ВЧ-накачки») на термінальних пристроях підсистеми керування АТС	К____
Ф08/РЕС\ВМ/ВЧ\ЕМ	Реєстрація випромінювання електромагнітних полів, що створюються в процесі генерації сигналів сторонніх ВЧ-коливань («ВЧ-накачки»)	К____
Ф08/МОН\АЕ\АЛ\А	Моніторинг сигналів побічних акусто-електричних перетворень на прикінцевих пристроях аналогових абонентських ліній	К____
Ф08/МОН\АЕ\ТЛ\СК	Моніторинг сигналів акусто-електричних перетворень на термінальних пристроях підсистеми керування станцією	К____
Ф08/МОН\АЕ/І/А\АЛ\Ц	Моніторинг аналогових інформативних складових акусто-електричних перетворень на прикінцевих пристроях цифрових абонентських ліній	К____
Ф08/МОН\СГ/ВЧ\АЛ\Ц	Моніторинг сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях цифрових абонентських ліній зв'язку	К____
Ф08/МОН\СГ/ВЧ\АЛ\А	Моніторинг сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях аналогових абонентських ліній зв'язку	К____
Ф08/МОН\СГ/ВЧ\ТЛ\СК	Моніторинг сигналів ВЧ-коливань («ВЧ-накачки») на термінальних пристроях підсистеми керування АТС	К____
Ф08/МОН\ВМ/ВЧ\ЕМ	Моніторинг випромінювання електромагнітних полів, що створюються в процесі генерації сигналів сторонніх ВЧ-коливань («ВЧ-накачки»)	К____
Ф08/ОСЛ\АЕ\АЛ\А	Ослаблення сигналів побічних акусто-електричних перетворень на прикінцевих пристроях аналогових абонентських ліній	К____

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф08/ОСЛ\АЕ\ТЛ\СК	Ослаблення сигналів акусто-електричних перетворень на термінальних пристроях підсистеми керування станцією	К____
Ф08/ОСЛ\СГ/ВЧ\АЛ\Ц	Ослаблення сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях цифрових абонентських ліній зв'язку	К____
Ф08/ОСЛ\СГ/ВЧ\ТЛ\АЛ\А	Ослаблення сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях аналогових абонентських ліній зв'язку	К____
Ф08/ОСЛ\СГ/ВЧ\ТЛ\СК	Ослаблення сигналів ВЧ-коливань («ВЧ-накачки») на термінальних пристроях підсистеми керування АТС	
Ф08/ОСЛ\ВМ/ВЧ\ЕМ	Ослаблення випромінювання електромагнітних полів, що створюються в процесі генерації сигналів сторонніх ВЧ-коливань («ВЧ-накачки»)	К____
Ф08/МСК\АЕ\АЛ\А	Маскування сигналів побічних акусто-електричних перетворень на прикінцевих пристроях аналогових абонентських ліній	К____
Ф08/МСК\АЕ\ТЛ\СК	Маскування сигналів акусто-електричних перетворень на термінальних пристроях підсистеми керування станцією	К____
Ф08/МСК\СГ/ВЧ\АЛ\Ц	Маскування сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях цифрових абонентських ліній зв'язку	К____
Ф08/МСК\СГ/ВЧ\АЛ\А	Маскування сигналів ВЧ-коливань («ВЧ-накачки») на прикінцевих пристроях аналогових абонентських ліній зв'язку	К____
Ф08/МСК\СГ\ТЛ/ВЧ\СК	Маскування сигналів ВЧ-коливань («ВЧ-накачки») на термінальних пристроях підсистеми керування АТС	К____
Ф08/МСК\ВМ/ВЧ\ЕМ	Маскування випромінювання електромагнітних полів, що створюються в процесі генерації сигналів сторонніх ВЧ-коливань («ВЧ-накачки»)	К____
9 Підсистема захисту від якісної недостатності інформаційно уразливих режимів, функцій і послуг, що надаються АТС		
Ф09/НТР\КВ\ІУ	Нейтралізація каналів витоку інформації в інформаційно уразливих режимах, функціях і послугах АТС	КЦ___
Ф09/КТР\ЦЛ\ЗЗ\ІУ	Контроль цілісності засобів захисту від якісної недостатності інформаційно уразливих режимів, функцій і послуг АТС	_Ц___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф09/ВЯВ\МА\ІУ	Виявлення, сигналізація, реєстрація моментів активізації інформаційно уразливих режимів, функцій і послуг АТС	___С_
Ф09/ПТД\НК\РР/ІУ	Наявність засобів протидії несанкціонованому користуванню ресурсами АТС у інформаційно уразливих режимах, функціях і послугах АТС	____Р
10 Підсистема захисту від збоїв та відмов у роботі АТС		
Ф10/ЗРЧ\СК	Наявність підвищених зручностей користування для персоналу АТС	__Д__
Ф10/ЗРЧ\АЛ	Наявність підвищених зручностей користування для абонента	__Д__
Ф10/ЗМН\ЗБ	Використання засобів зменшення інтенсивності відмов	__Д__
Ф10/НМР/С/ТЗ	Використання структурної надмірності (наприклад, використання чотирьохкратної логіки з переплетеннями)	__Д__
Ф10/НМР/І/ПЗ	Використання інформаційної кодової надмірності (наприклад, використання кодів із виявленням і виправленням помилок)	__Д__
Ф10/НМР/СГ/ТЗ’ПЗ	Використання сигнальної надмірності (наприклад, використання багатопозиційних методів модуляції/демодуляції сигналів)	__Д__
Ф10/НМР/ТЗ/А	Використання апаратурної алгоритмічної надмірності (для виявлення та усунення наслідків збоїв)	__Д__
Ф10/НМР/ПЗ’Ф	Використання програмної і (або) функціональної надмірності	__Д__
Ф10/НМР/ПЗ/А	Використання алгоритмічної надмірності програм (наприклад, використання «нечутливих» алгоритмів)	__Д__
Ф10/НМР/ПЗ/С	Використання структурної надмірності програм (наприклад, за допомогою використання методу контрольних функцій і т. ін.)	__Д__
Ф10/ВКР/ПЗ/С	Використання структурних методів програмування	__Д__
Ф10/ВКР/ПЗ/Д	Використання доказових методів програмування	__Д__
Ф10/ВКР/ПЗ/М	Використання модульності програмного забезпечення	__Д__
Ф10/ТСТ\ПЗ/С	Структурні методи тестування програмного забезпечення	__Д__

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф10/ТСТ\ПЗ'ТЗ	Системне тестування програмно-технічних засобів	__Д__
Ф10/ПТД\ПЗ\Щ	Наявність захисту від можливості завантаження позаштатного програмного забезпечення	__Д__
Ф10/ПТД\ТЗ\ЗК	Наявність конструкції, що утруднює можливість установлення закладних пристроїв (мінімальний вільний простір, компаунди, запаяні кожухи і т. ін.)	__Д__
Ф10/ПТД\М/РЕ\ЕУ	Наявність механічних засобів, що обмежують фізичний доступ до елементів устаткування АТС (нерозбірні зовні шафи, замкові пристрої і т. ін.)	__Д__
Ф10/ВЯВ\НК\ЕУ	Виявлення і реєстрація спроб несанкціонованого доступу до елементів устаткування	__Д__
11 Підсистема захисту від загроз у системах збереження інформації на фізичних носіях		
Ф11/ЗНЩ\РР\І/НК/ФН	Знищення (стирання) інформації, збереженої на фізичних носіях, після виявлення спроб несанкціонованого доступу до неї	КЦ___
Ф11/КТР\ЦЛ\ЗЗ	Наявність засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів бази захисту АТС	_Ц___
Ф11/КТР\ЦЛ\ПЗ	Наявність засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів програмного забезпечення АТС	_Ц___
Ф11/РДО\ФН	Розмежування правил доступу до інформації, збереженої на фізичних носіях	КЦ___
Ф11/ШФР\ФН	Шифрування інформації, збереженої на фізичних носіях	КЦ___
Ф11/КТР\ФН	Контроль інформації, збереженої на фізичних носіях	_Ц___
12 Система ліквідації наслідків реалізованих загроз інформації на АТС		
Ф12/ТСТ/П\НВ\ЗХ	Наявність режиму повного циклу тестування АТС у процесі відновлення захищеності у разі порушення безперервності захисту	_Ц___
Ф12/НОВ\ЗЗ\ РР\І	Можливість відновлення бази захисту після реалізованих загроз інформаційним ресурсам АТС	_Ц___
Ф12/ОХР\ТЗ'ФН	Наявність фізичної охорони штатного і додаткового устаткування АТС і носіїв інформації	_Ц___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф12/ЗМН\ТВ\ПЗ’ТЗ	Забезпечення зменьшення середнього часу відновлення програмно-технічних засобів після відмов	__Д__
Ф12/КТР\МВ	Забезпечення діагностики системи (пошуку місця відмови)	__Д__
Ф12/КТР\ПЗ	Забезпечення програмно-логічного контролю програмного забезпечення	__Д__
Ф12/КТР/М\ПЗ’ТЗ	Забезпечення апаратного оперативного контролю програмно-технічних засобів АТС	__Д__
Ф12/ВКР/ЕУ/З	Використання наявних запасних елементів устаткування	__Д__
Ф12/РКФ\НТР\ЗБ	Забезпечення реконфігурації системи для нейтралізації наслідків відмов елементів устаткування	__Д__
Ф12/ІЗЛ\ЗБ	Забезпечення ізоляції елементів системи, що відмовили	__Д__
Ф12/РДЛ\РР\Т’П	Забезпечення просторово-часового рознесення елементів системи, що резервуються	__Д__
Ф12/НТР\НП\ПЗ’ТЗ	Забезпечення відмовостійкості за рахунок використання засобів активної нейтралізації джерел негативних впливів на програмно-технічні засоби АТС після їх виявлення і реєстрації	__Д__
Ф12/ОРГ\ТО	Наявність системи технічного обслуговування та ремонту АТС	__Д__
Ф12/АНЛ\ЗБ	Наявність системи збору, зберігання і аналізу інформації про збої та відмови	__Д__
Ф12/НМР/ТЗ/Т	Забезпечення відмовостійкості за рахунок використання методів одержання тимчасової надмірності	__Д__
Ф12/РЕЗ/ТЗ	Забезпечення відмовостійкості за рахунок використання елементів апаратного резервування	__Д__
Ф12/ОРГ\ВС/ФЕ	Забезпечення відмовостійкості за рахунок використання елементів однакового функціонального призначення, але різних за фізичною природою функціонування	__Д__
13 Система керування засобами ТЗІ		
Ф13/КТР\КФ\ПЗ’ТЗ	Наявність механізмів спостереження за змінами конфігурації програмно-технічних засобів підсистеми керування АТС	_Ц___

Терм, що позначає ФПЗ	Визначення ФПЗ	Перелік видів загроз, яким ФПЗ протидіє
Ф13/КТР\КФ\ПЗ'ТЗ\ПК	Наявність механізмів спостереження за змінами конфігурації програмно-технічних засобів підсистеми комутації абонентських і з'єднувальних ліній АТС	_Ц___
Ф13/КТР\КФ\ЗЗ	Наявність механізмів спостереження за змінами конфігурації бази захисту АТС	_Ц___

6 Специфікації рівнів стійкості механізмів захисту

Згідно з НД ТЗІ 2.7-001-99 на стадії розробки та реалізації проекту КЗМЗ, а також на стадії оцінювання коректності реалізації створеного КЗМЗ мають бути визначені рівні стійкості засобів та механізмів захисту, які реалізують ФПЗ, що віднесені до моделі захисту.

Рівень стійкості механізма захисту позначається однією цифрою від 1 до 3. При цьому розуміється, що:

1 – позначає мінімальний (базовий) рівень стійкості механізмів захисту;

2 – позначає середній рівень стійкості механізмів захисту;

3 – позначає високий рівень стійкості механізмів захисту.

Механізми захисту, що реалізують певну ФПЗ, можуть відрізнятись між собою як за ступенем ефективності реалізації цієї функції (тобто, за ступенем досконалості реалізації стосовно можливих "слабких місць" у захисті), так і за ступенем стійкості механізму стосовно спроб його безпосереднього злому.

У процесі оцінки коректності реалізації КЗМЗ необхідно переконатися, що кожна ФПЗ, яка включена до моделі захисту інформаційних ресурсів АТС, реалізується на практиці з рівнями стійкості механізмів захисту не меншими зазначених у документації техно-робочого проекту, також необхідно підтвердити, що всі запроектовані механізми захисту реально діють на оцінюваній АТС відповідно до нормованих специфікацій рівнів стійкості механізмів захисту. Такі нормовані специфікації рівнів стійкості механізмів захисту наведені в цьому розділі.Надані специфікації рівнів стійкості механізмів захисту структуровані щодо основних видів загроз інформаційним ресурсам АТС (див. НД ТЗІ 1.1-001-99).

Специфікації базового (мінімального), середнього і високого рівнів стійкості механізмів захисту, що реалізують ФПЗ, наведені у таблиці 7.

Таблиця 7 Специфікації рівнів стійкості механізмів захисту

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф01/РДО/Д/МО\ПЦ\СК Ф01/РДО/Д/АЛ\ПС	
1 Керування доступом здійснюється за допомогою імен суб'єктів та ідентифікаторів об'єктів з використанням довірчих ПРД.	1,2
2 Механізм керування доступом містить в собі множину засобів підтримки обмежень доступу на індивідуальному рівні (на рівні окремих суб'єктів).	1,2
3 Передача прав на доступ здійснюється на рівні суб'єкта або групи суб'єктів.	1,2

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
4 Механізм керування доступом повинен підтримувати шість або більше атрибутів прав доступу (наприклад, запис, читання, виконання і т. ін.).	1,2
5 Використовується стратегія мінімуму повноважень суб'єктів шляхом логічної ізоляції ресурсів, що виділяються суб'єктам доступу.	2
6 Керування доступом дозволяє: – згруповувати суб'єкти; – розподіляти об'єкти між суб'єктами; – обмежувати поширення прав доступу; – надавати дозвіл на доступ (санкціонувати доступ) у статичному режимі.	2
7 Керування доступом дає можливість деталізувати розподіл прав на доступ до рівня окремого суб'єкта.	2
8 Підтримується вісім або більше атрибутів прав доступу	2
Ф01/РДО/Н\МО\ПЦ\СК Ф01/РДО/Н/АЛ\ПС	
1 Використовуються мандатні ПРД між ієрархічними рівнями повноважень суб'єктів та ієрархічними дозволеними рівнями доступу до об'єктів АТС.	1
2 Керування доступом здійснюється за допомогою ідентифікаторів суб'єктів і маркерів об'єктів відповідно до матриці доступу.	1
3 Керування доступом дозволяє: – згруповувати суб'єкти; – розподіляти об'єкти між суб'єктами; – обмежувати поширення прав доступу; – видавати дозвіл на доступ (санкціонувати доступ) у статичному режимі.	1
4 Керування доступом дає можливість деталізувати розподіл прав на доступ до рівня окремого суб'єкта.	1
5 Підтримується вісім або більше атрибутів прав доступу.	1
6 Суб'єкт доступу має можливість запросити і одержати від бази захисту АТС інформацію про класифікаційний маркер створеного ним об'єкта.	1
Ф01/РДО/Д'Н/МО\ПЦ\СК Ф01/РДО/Д'Н/АЛ\ПС	
1 Використовується змішана стратегія керування доступом: мандатний принцип розподілу доступу між ієрархічними рівнями повноважень суб'єктів і ієрархічними дозволеними рівнями доступу до об'єктів АТС, а також посилений довірчий принцип розподілу доступу з використанням стратегії мінімуму повноважень всередині кожного дозволеного рівня доступу до об'єктів.	1,2,3
2 Механізм керування доступом забезпечує можливість підтримки не менше чотирьох рівнів повноважень суб'єктів, не менше восьми ієрархічних дозволених рівнів доступу до об'єктів і не менше 64-х класів повноважень суб'єктів і дозволених рівнів доступу всередині кожного дозволеного ієрархічного рівня.	1,2,3
3 База захисту АТС керує розподілом доступу усередині дозволеного ієрархічного рівня доступу до об'єктів АТС за іменами суб'єктів з використанням стратегії мінімуму повноважень відповідно до матриці доступу.	1,2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
4 Керування доступом дозволяє уповноваженим суб'єктам: – згруповувати суб'єкти; – розподіляти об'єкти за суб'єктами; – обмежувати поширення прав доступу; – надавати дозвіл (санкціонувати) на доступ у статичному режимі.	1,2,3
5 Керування доступом дає можливість деталізувати розподіл до рівня окремого суб'єкта.	1,2,3
6 Деталізація прав доступу повинна включати вісім або більше атрибутів.	1,2,3
7 Суб'єкт повинен мати можливість запросити і одержати від бази захисту АТС інформацію про класифікаційний маркер створеного ним об'єкта.	1,2,3
8 База захисту АТС повинна негайно повідомляти суб'єктам в інтерактивному режимі про будь-які зміни рівня їхніх повноважень.	2,3
9 Стратегія захисту має бути з обліком ідентифікованих каналів.	3
10 Здійснюється керування потоками інформації за допомогою міток конфіденційності; при цьому дозволений рівень доступу до пристроїв нагромадження інформації повинний бути не нижче дозволених рівнів доступу до записаної на них інформації	3
Ф01/МРК\Н\РР\І Ф01/МРК\Д'Н\РР\І	
1 Маркування об'єктів доступу здійснюється на рівні файлової структури операційної системи з підтримкою шести і більше атрибутів прав доступу, включаючи обмеження прав доступу тільки читання, тільки виконання доступу до системних ресурсів, ресурсів загального користування АТС, ресурсів суб'єктів.	1
2 Маркування об'єктів доступу здійснюється на рівні операційної системи і комунікаційних протоколів з підтримкою восьми і більше атрибутів прав доступу.	1,2
3 Механізм маркування повинен підтримувати не менше 64-х класів повноважень суб'єктів і дозволених рівнів доступу до об'єктів для підтримки стратегії мінімуму повноважень. Всі маркери об'єктів повинні містити інформацію про ієрархічні рівні доступу до об'єкта і класи його доступу всередині кожного ієрархічного рівня.	1,2
4 Підтримка програмно реалізованих логічних процедур контролю цілісності маркерів об'єктів доступу на всіх етапах передачі або прийому інформації.	3
5 Підтримка в маркерах об'єктів доступу атрибута обмеження часу життя переданої і (або) прийнятої інформації.	1,2
6 Підтримка технічних засобів маркування об'єктів доступу на АТС	1,2
7 Можливість перетворення форми уявлення маркера адекватно перетворенням інформації на об'єктах, що пов'язані з цим маркером.	2,3
8 Підтримка в маркерах для фізичних пристроїв атрибута дозволених рівнів доступу до цих пристроїв.	2,3
9 Підтримка цілісності маркерів протоколами комунікаційних каналів.	2,3
10 Підтримка процедур контролю адекватності рівня фізичних пристроїв класифікаційному рівню інформації.	2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
11 Маркування всіх сторінок читабельного тексту.	2,3
12 Підтримка процедур перевірки адекватності читабельної форми маркера внутрішній формі його уявлення.	2,3
13 Підтримка для кожного маркера об'єктів АТС списків доступу.	2,3
Підтримка для маркерів фізичних пристроїв атрибутів максимального і мінімального рівнів доступу.	3
Ф01/ІЗЛ\ЗЗ Ф01/ІЗЛ\СЗ Ф01/ІЗЛ\РР\Г Ф02/ІЗЛ\ЗВ/ПЗ'ТЗ/Ш Ф04/ІЗЛ\ОД\ЗВ\ЕУ Ф05/ІЗЛ\ОД\ЗВ\ПЦ Ф06/ІЗЛ\ОД\ЗК Ф06/ІЗЛ\СЗ/ПЗ	
1 Доступ до об'єктів ізолюється на логічному рівні за допомогою програмних засобів.	1
2 Доступ до об'єктів ізолюється за допомогою програмно-технічних засобів.	2
3 Доступ до об'єктів ізолюється за допомогою технічних засобів	3
Ф01/ПТР/ПС\УО	
1 Підтримка режиму і функцій адміністратора АТС.	1
2 Підтримка режиму і функцій виділеної системної консолі.	1
3 Реалізується підтримка поділу режимів і функцій адміністратора АТС і адміністратора безпеки АТС. Адміністратор безпеки повинен мати свій термінал і необхідні засоби оперативного контролю і впливу на захищеність АТС.	2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
4 Забезпечується технічна підтримка таких спеціалізованих функцій для адміністратора безпеки як: – реєстрація входу/виходу суб'єктів доступу в систему/із системи або завантаження/зупинки системи; – реєстрація видачі друкарських (графічних) документів на «тверду копію»; – реєстрація запуску/завершення всіх програм і процесів (завдань, задач) на АТС; – реєстрація спроб доступу суб'єктів (у тому числі, активних програмних засобів) до логічних об'єктів, що захищаються (програм, процесів, каталогів, файлів, задач, завдань); – реєстрація спроб доступу суб'єктів (у тому числі, активних програмних засобів) до фізичних об'єктів (пристроїв друку, фізичних пристроїв пам'яті, віддалених терміналів, каналів зв'язку та ін.); – реєстрація змін повноважень суб'єктів доступу і статусу об'єктів доступу; – реєстрація всіх знову створюваних суб'єктів, суб'єктів, що видаляються та об'єктів доступу; – облік усіх носіїв інформації, що захищаються, за допомогою їхнього маркування; – сигналізація спроб порушення захисту АТС; – структуризація й аналіз даних про стан ахисту інформаційних ресурсів на АТС; – запуск (в тому числі, програмно-керований) тестового і діагностичного забезпечення бази захисту АТС.	2,3
5 Адміністратор безпеки АТС повинний мати засоби моніторингу, що забезпечують безупинний контроль у реальному часі поточного стану захищеності АТС.	3
6 Реалізується механізм персональної автентифікації і реєстрації в системі, аудиту дій адміністратора безпеки АТС.	3
Реалізується обмежений перелік ідентифікованих функцій для адміністратора безпеки, зокрема тільки таких функцій, що безпосередньо впливають на ефективність захисту АТС	3
Ф01/РДО\ОД\СД	
1 Використовуються програмні засоби логічного поділу об'єктів між суб'єктами доступу.	1
2 Використовуються технічні засоби логічного поділу об'єктів між суб'єктами з обліком розходження повноважень суб'єктів і атрибутів прав доступу до об'єктів (наприклад, шляхом використання апаратних механізмів прямого доступу або сегментування пам'яті).	2
3 Використовуються технічні засоби фізичного розподілу об'єктів між суб'єктами з обліком розходжень повноважень суб'єктів, рівнів конфіденційності логічних і фізичних пристроїв (зокрема, каналів зв'язку) та атрибутів прав доступу до об'єктів (наприклад, фізична реалізація системного і базового програмного забезпечення АТС на ПЗУ)	3
Ф01/ВИК\ЗР'ЗМ\ПЗ\Ш	
1 Виключення з операційного середовища АТС компіляторів, трансляторів, в'юверів, дебагерів і т. ін..	1,2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
2 Наявність тільки повністю штатного набору експлуатаційного програмного забезпечення.	2,3
3 Реалізація захисту від можливості завантаження нештатного програмного забезпечення	1,2,3
Ф01/БЛК\ОД Ф02/БЛК\ОД\ЗВ Ф04/БЛК\ОД\ЗВ\ЕУ Ф05/БЛК\ОД\ЗВ\ПЦ Ф06/БЛК\ОД\ЗК	
1 Використання програмно-технічних засобів блокування об′єктів доступу у разі НСД до ресурсів АТС або позаштатних впливів на програмне та(або) технічне забезпечення АТС	2,3
Ф01/СКР\РР\І\АЛ Ф02/СКР\РР\І\АЛ Ф04/СКР\РР\І\АЛ Ф05/СКР\РР\І\АЛ	
1 Доступ суб’єктів до операцій скремблювання і до відповідних ключів контролюється механізмами керування доступом.	1
2 Використовується скремблювання за допомогою програмно-технічних засобів всієї уразливої технологічної і (або) службової інформації, що записується на носії даних у каналах зв’язку, які спільно використовуються різними суб’єктами доступу, а також на зйомні портативні носії даних для збереження за межами сеансів роботи санкційонованих суб’єктів доступу. У цьому випадку повинне виконуватися примусове очищення областей зовнішньої пам’яті, що містили раніше незашифровану інформацію.	2
3 Доступ суб’єктів до операцій скремблювання і до відповідних ключів контролюється за допомогою підсистеми керування доступом, що використовує механізми захисту із середніми і(або) високими рівнями стійкості.	2,3
4 Використовується апаратне скремблювання всієї уразливої інформації в підсистемі керування АТС.	3
5 Криптостійкість використовуваного алгоритму скремблювання і умови застосування системи скремблювання, що використовується, повинні бути або формально визначені, або піддані ретельному аналізу з боку уповноваженого національного органа	3
Ф01/ТСТ/Т\ЦЛ\КФ\ПЗ’ТЗ Ф01/ТСТ/Т\ЦЛ\ЗЗ Ф01/ТСТ/Т\ЦЛ\ДЗ	
1 Використовується перевірка цілісності конфігурації за наявністю імен і(або) ідентифікаторів компонент у каталогах і директоріях системи.	1,2,3
2 Використовується перевірка цілісності за контрольними сумами компонентів системи.	2
3 Використовується перевірка цілісності за допомогою спеціалізованих технічних засобів із високою спроможністю виявлення порушень цілісності	3
Ф01/ЗНЩ\ОП\ОД	
1 Очищення областей пам’яті об’єктів перед їх повторним використанням за допомогою механізмів розподілу ресурсів АТС	1,2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф01/ЗНЩ\ОД Ф02/ЗНЩ\ОД\ЗВ Ф04/ЗНЩ\ОД\ЗВ\ЕУ Ф05/ЗНЩ\ОД\ЗВ\ПЦ Ф06/ЗНЩ\ОД\ЗК Ф11/ЗНЩ\РР\І/НК/ФН	
1 Використовуються програмні та (або) технічні засоби знищення інформації та (або) фізичних носіїв інформації. 2 Використовуються методи знищення інформації та (або) фізичних носіїв інформації, що засновані на багаторазовому запису на місце знищеної інформації з певними ймовірностними характеристиками та (або) використання спеціальних пристроїв знищення фізичних носіїв інформації. 3 Використовуються потужні методи знищення інформації та (або) фізичних носіїв інформації (див. наприклад, вище п.2) із перевіркою і фіксацією причин знищення та контролем доступу до засобів знищення	1 2 3
Ф01/АНЛ/ПР\СК Ф01/АНЛ/ПР\АЛ	
1 Реалізується протокол простої незахищеної ідентифікації й автентифікації (впізнання, перевірки істинності) під час входу суб’єктів у систему за паролем умовно-постійної дії довжиною не менше ніж шість літеро-цифрових символів. 2 Реалізуються механізми захисту даних автентифікації від доступу з боку абонентів АТС. 3 Реалізується протокол простої захищеної ідентифікації й автентифікації у випадку входу у систему за допомогою атестованих прграмно-технічних засобів з використанням пароля умовно-постійної дії довжиною не менше восьми літеро-цифрових символів. 4 Реалізуються механізми захисту даних автентифікації від неуповноважених суб’єктів доступу. 5 Забезпечується підтримка нерозривного зв’язку унікального ідентифікатора користувача АТС з усіма його діями на АТС	1 1 2 2 2
Ф01/АУД\СК Ф01/АУД\АЛ Ф13/КТР\КФ\ПЗ’ТЗ Ф13/КТР\КФ\ПЗ’ТЗ\ПК Ф13/КТР\КФ\ЗЗ	

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
1 Механізм аудиту повинен підтримувати реєстрацію в системному журналі всіх подій, що пов'язані з ідентифікацією і доступом користувачів підсистеми керування станцією до об'єктів АТС. Для кожної події, що реєструється, аудиторський запис повинен включати: – дату і час події; – ім'я і, можливо, ідентифікатор користувача, який пред'явлений при спробі доступу; – тип події; – код завершення події; – ім'я і, можливо, маркер переданого об'єкта або об'єкта, що знищується.	1
2 Механізм аудиту повинен підтримувати реєстрацію в системному журналі всіх подій, пов'язаних з ідентифікацією і доступом персоналу станції (наприклад, телефоніcток) до баз даних, що містять конфіденційну інформацію абонентів і про абонентів. Для кожної події, що реєструється, аудиторський запис повинен включати: – дату і час події; – ідентифікатор і, можливо, ім'я суб'єкта; – тип запиту; – код завершення запиту; – ім'я і, можливо, маркер запитуваного об'єкта.	1
3 Реалізуються процедури і функції контролю за діями користувачів із боку персоналу АТС: – реєстрація результатів кожного запиту на автентифікацію; – реєстрація подій щодо передачі об'єктів в адресний простір користувачів (наприклад, ініціалізація програм, процесів і т. ін.); – реєстрація подій щодо знищення об'єктів; – реєстрація дій персоналу й адміністратора АТС, а також інших подій, що змінюють стан бази захисту.	1
4 Реалізуються процедури і функції контролю за діями суб'єктів доступу до конфіденційної інформації абонентів з боку персоналу і (або) адміністратора АТС: – реєстрація результатів кожного запиту на автентифікацію; – реєстрація подій щодо передачі об'єктів в адресний простір суб'єктів доступу; – реєстрація подій щодо знищення об'єктів; – реєстрація будь-яких подій, що змінюють стан бази захисту АТС.	1
5 Реалізуються на логічному рівні процедури обмеження доступу до аудиторської інформації. Доступ на читання і знищення аудиторської інформації повинен бути обмежений тільки колом уповноважених осіб, що контролюють аудиторську інформацію.	1,2

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
6 Механізм аудиту повинен підтримувати реєстрацію в базі захисту АТС усіх подій, пов'язаних із процесами ідентифікації, аутентифікації і розподілу доступу між суб'єктами і об'єктами в підсистемі керування станцією. Для кожної події, що реєструється, аудиторський запис повинен включати: – дату і час події; – адреси активного терміналу; – ідентифікатор користувача, пред'явлений при спробі доступу; – тип події; – код завершення опрацювання події; – ім'я і маркер обмеження доступу до об'єкту, що знищується або передається.	2,3
7 Реалізуються процедури і функції контролю за діями користувачів з боку системного адміністратора АТС і (або) адміністратора безпеки АТС: – реєстрація результатів кожного запиту на автентифікацію, включаючи дані про джерело надходження запиту; – реєстрація подій щодо передачі об'єктів в адресний простір користувачів (наприклад, ініціалізація програм, процесів і т. ін.); – реєстрація подій щодо видалення об'єктів з адресного простору користувача; – реєстрація дій персоналу, системного адміністратора, адміністратора безпеки АТС, а також інших подій, що змінюють стан бази захисту або порушують безперервність захисту (аварійна зупинка, програмна зупинка і т. ін.).	2,3
8 Механізм аудиту повинен підтримувати реєстрацію в базі захисту АТС всіх подій, пов'язаних з процесами автентифікації і розподілу доступу між персоналом і абонентами станції, з одного боку, і такими об'єктами доступу, як конфіденційні дані абонентів і про абонентів, послуги зв'язку, сервісні та інші послуги, що надаються станцією, з іншого боку. Для кожної події, що реєструється, аудиторський запис повинен включати: – дату і час події; – адреси активного терміналу, телефонного комутатора або абонентського прикінцевого пристрою; – ідентифікатор суб'єкта; – тип події або запиту; – код завершення опрацювання події або запиту; – ім'я і маркер обмеження доступу до об'єкту, що знищується або передається.	2,3
9 Забороняється доступ до аудиторської інформації на фізичному рівні з боку телефонних комутаторів і абонентських прикінцевих пристроїв. Доступ на читання і знищення аудиторської інформації здійснюється тільки з боку системних терміналів і обмежується тільки колом осіб, що контролюють аудиторську інформацію.	2,3
10 Повинна здійснюватися реєстрація видачі друкарських (графічних) документів на «тверду» копію. Видача повинна супроводжуватися автоматичним маркуванням кожного листа (сторінки) документа. Разом із видачею документа повинна автоматично оформлятися облікова картка документа з вказівкою дати видачі документа, облікових реквізитів документа, короткого змісту і рівня конфіденційності документа, ідентифікатора суб'єкта, що видав документ, кількості сторінок і копій документа.	2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
11 Система аудиту повинна реєструвати всі події, що пов'язані з порушенням маркування читабельного виводу (вивід на екран, друкувальний пристрій і т. ін.).	2,3
12 Здійснюється реєстрація запуску і завершення всіх програм і процесів (задач, завдань) на АТС.	2,3
13 Здійснюється реєстрація спроб доступу програмних засобів (програм, процесів, задач, завдань) до всіх файлів, що захищаються.	2,3
14 Здійснюється реєстрація спроб доступу до логічних об'єктів доступу АТС, що захищаються (програм, томів, каталогів, файлів, записів, полів записів).	2,3
15 Здійснюється реєстрація спроб доступу до фізичних об'єктів доступу на АТС, що захищаються (терміналів, процесорів, вузлів, зовнішніх пристроїв, каналів і ліній зв'язку).	2,3
16 Система аудиту повинна реєструвати будь-які зміни рівнів і (або) параметрів комунікаційних каналів і (або) зовнішніх (периферійних) пристроїв АТС.	2,3
17 Здійснюється автоматичний облік створюваних або активізуємих файлів томів, каталогів, областей ОЗП, а також фізичних пристроїв, що підлягають захисту або використовуються під час обробки захищаємої інформації, за допомогою їх додаткового маркування.	2,3
18 Механізм аудиту повинен підтримувати реєстрацію подій, пов'язаних з використанням ідентифікованих (тобто, включених у модель загроз) схованих каналів пам'яті.	3
19 Механізм аудиту повинен підтримувати реєстрацію подій, пов'язаних з використанням ідентифікованих (тобто, включених у модель загроз) схованих таймерних каналів.	3
20 Реалізуються процедури аналізу аудиторської інформації, що накопичується в процесі функціонування АТС у реальному масштабі часу з метою виявлення появи подій, що являють собою загрозу для інформації на АТС (наприклад, перевищення кількості зафіксованих подій деякого граничного значення, що може викликати підозру про можливу спробу проникнення і т. ін.)	3
Ф01/КТР\ШС	
1 Підтримка на логічному рівні індикації на системній консолі АТС поточного стану процесів на рівні прикладних систем.	1
2 Програмно-технічна підтримка індикації на системній консолі АТС і (або) на дисплейних пристроях телефонних комутаторів дій абонентів у разі замовлення конкретних послуг зв'язку і (або) сервісних послуг.	1
3 Програмно-технічна підтримка індикації на системної консолі АТС поточного стану процесів на рівні базових програмних засобів і прикладних систем.	2
4 Підтримка індикації на системній консолі дій персоналу з керування й обслуговування станції.	2,3
5 Підтримка на технічному рівні індикації на системних консолях поточного стану процесів на всіх прошарках технологічного середовища АТС (на рівні операційної системи, базових програмних засобів, прикладних систем).	3
6 Підтримка індикації на системній консолі і (або) на дисплейних пристроях телефонних комутаторів дій абонентів щодо замовлення конкретних послуг зв'язку і (або) сервісних послуг	3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф01/ТСТ\ЦЛ\ПЗ’ТЗ Ф04/ТСТ\ЦЛ\ЗЗ\ЗВ\ЕУ	
1 Використовуються програмні засоби спостереження за процесами, пов’язаними з перевіркою автентичності (цілісності) програмно-технічних засобів АТС. 2 Використовуються програмно-технічні засоби спостереження за процесами, пов’язаними з перевіркою автентичності (цілісності) програмно-технічних засобів АТС. 3 Використовуються програмно-технічні засоби безперервного спостереження за процесами, пов’язаними з перевіркою автентичності (цілісності) програмно-технічних засобів АТС	1 2 3
Ф01/ПТР/ПЗ/АН\АВ	
1 Реалізуються програмні засоби періодичного аналізу аудиторських вибірок для уповноважених суб’єктів або системного адміністратора АТС. 2 Реалізуються програмні засоби періодичного аналізу аудиторських вибірок для адміністратора безпеки АТС. 3 Реалізуються програмні і (або) програмно-технічні засоби безперервного в часі аналізу аудиторських вибірок для адміністратора безпеки АТС	1 2 3
Ф01/ПТР/ПЗ\ЗЗ Ф02/ТСТ/ЗС\ЗЗ\ЗВ Ф04/ТСТ\ЗЗ\ЗВ\ЕУ Ф05/ТСТ\ЗЗ\ЗВ\ПЦ Ф06/ТСТ/ЗС\ЗЗ\ЗК	
1 Використовуються засоби спостереження за реалізаціями процедур періодичного тестування в повному обсязі механізмів захисту АТС уповноваженим персоналом на відповідність описовим системним специфікаціям вищого рівня. 2 Реалізуються процедури періодичного тестування в повному обсязі механізмів захисту АТС уповноваженим персоналом на відповідність описовим системним специфікаціям вищого рівня і на стійкість системи захисту в цілому стосовно тестів на проникнення. 3 Реалізуються процедури періодичного тестування бази захисту АТС в повному обсязі і всіх її механізмів уповноваженим персоналом на відповідність формальним специфікаціям механізмів захисту і формальним специфікаціям цілісної системи захисту	1 2 3
Ф01/ВЯВ/ТЛ\НК Ф02/ВЯВ\ЗВ/ПЗ’ТЗ/Ш Ф04/ВЯВ\ЗВ/ПЗ’ТЗ\ЕУ Ф05/ВЯВ\ЗВ/ПЗ’ТЗ\ПЦ	
1 Використовуються засоби сигналізації і реєстрації спроб НСД на термінал порушника. 2 Використовуються засоби сигналізації і реєстрації спроб НСД на терміналах порушника і системного адміністратора. 3 Використовуються програмно-технічні засоби сигналізації і реєстрації будь-яких спроб НСД на термінал адміністратора безпеки і спроб НСД (із числа заздалегідь запрограмованих видів НСД) на терміналах порушника	1 2 3
Ф01/ІЗЛ\ОП\СД	
1 Логічна ізоляція областей пам’яті.	1

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
2 Програмна ізоляція областей пам’яті. 3 Апаратна ізоляція областей пам’яті.	2 3
Ф01/ШФР\РР\І\СК Ф01/ШФР\РР\І\АЛ Ф02/ШФР\РР\І\СК Ф02/ШФР\РР\І\АЛ Ф04/ШФР\РР\І\СК Ф04/ШФР\РР\І\АЛ Ф05/ШФР\РР\І\СК Ф05/ШФР\РР\І\АЛ Ф06/ШФР\РР\І\СК Ф06/ШФР\РР\І\АЛ Ф11/ШФР\ФН	
1 Використовується шифрування за допомогою програмних засобів найбільш уразливої технологічної і (або) службової інформації на АТС, що записується на фізичні носії даних, а також на ущільнених каналах зв’язку. 2 Доступ суб’єктів до операцій шифрування і до відповідних ключів контролюється механізмами керування доступом. 3 Використовується шифрування за допомогою програмно-технічних засобів всієї уразливої технологічної і (або) службової інформації, що записується на носії даних у каналах зв’язку, які спільно використовуються різними суб’єктами доступу, а також на зйомні портативні носії даних для збереження за межами сеансів роботи санкційонованих суб’єктів доступу. У цьому випадку повинне виконуватися примусове очищення областей зовнішньої пам’яті, що містили раніше незашифровану інформацію. 4 Використовуються криптостійкі алгоритми шифрування, реалізовані атестованими криптографічними засобами. 5 Доступ суб’єктів до операцій шифрування і до відповідних ключів контролюється за допомогою підсистеми керування доступом, що використовує механізми захисту із середніми і(або) високими рівнями стійкості. 6 Використовується апаратне шифрування всієї уразливої інформації в підсистемі керування АТС. 7 Використовуються різні криптографічні ключі для шифрування інформації, що належить різним суб’єктам доступу (різним групам суб’єктів). 8 Криптостойкість використовуваного алгоритму шифрування і умови застосування системи шифрування, що використовується, повинні бути або формально визначені, або піддані ретельному аналізу з боку уповноваженого національного органа.	1 1 2 2,3 2,3 3 3 3
Ф01/НМР/РР/І Ф01/НМР/РР/М	
1 Використання простих методів введення апаратної надмірності (наприклад, шляхом застосування додаткових розрядів у розрядній сітці уявлення чисел в процесорних елементах і в елементах пам’яті для уявлення результатів підсумовування за модулем два і т. ін.) для контролю цілісності об’єктів доступу.	1
2 Використання вдосконалених методів введення апаратної надмірності (наприклад, заснованих на сигнатурному аналізі сигналів) для контролю цілісності об’єктів доступу.	2

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
3 Використання потужних методів введення апаратної надмірності (із високою спроможністю виявлення і виправлення) для контролю і забезпечення цілісності об'єктів доступу.	3
Ф01/ПТД\ЗЄ\Е Ф01/ПТД\ПС\Е	
1 Реалізуються на логічному рівні програмні механізми відвернення помилкових з'єднань на станції. 2 Реалізуються прграмно-технічні механізми відвернення помилкових з'єднань на станції. 3 Реалізуються технічні механізми відвернення помилкових з'єднань на станції.	1 2 3
Ф02/РДО/ПЦ/ПЗ'ТЗ/Ш\НМ	
1 Використовуються програмні засоби логічного розподілу об'єктів між суб'єктами доступу. 2 Використовуються технічні засоби логічного поділу об'єктів між суб'єктами з обліком розходження в повноваженнях суб'єктів і в атрибутах прав доступу до об'єктів (наприклад, шляхом використання апаратних механізмів прямого доступу або сегментування пам'яті). 3 Використовуються технічні засоби фізичного поділу об'єктів між суб'єктами з обліком розходжень у повноваженнях суб'єктів, у рівнях конфіденційності логічних і фізичних пристроїв (зокрема, каналів зв'язку) і в атрибутах прав доступу до об'єктів (наприклад, фізична реалізація системного і базового програмного забезпечення АТС на ПЗУ).	1 2 3
Ф02/ТСТ\ЦЛ\ЗЗ\ЗВ/Ш	
1 Використовуються програмні засоби спостереження за процесами, пов'язаними з перевіркою автентичності (цілісності) засобів захисту. 2 Використовуються програмно-технічні засоби спостереження за процесами, пов'язаними з перевіркою автентичності (цілісності) засобів захисту. 3 Використовуються програмно-технічні засоби безперервного спостереження за процесами, пов'язаними з перевіркою автентичності (цілісності) засобів захисту.	1 2 3
Ф02/ПТД/О\НК\АЛ	
1 Введення паролю на абонентську лінію.	1,2
Ф02/ВЯВ/О\НК\АЛ\Ц\Ш	
1 Використання індивідуальних засобів протидії несанкціонованому користуванню цифровою абонентської лінією АТС, заснованих на виявленні електричних відключень штатних цифрових абонентських прикінцевих пристроїв.	2
Ф02/ВЯВ/О\НК\АЛ\А	
1 Застосування індивідуальних засобів виявлення несанкціонованого користування аналоговою абонентською лінією АТС за допомогою штатного аналогового абонентського прикінцевого пристрою.	2
Ф02/ТСТ\ЗЗ\ЗВ Ф10/ТСТ\ПЗ'ТЗ	
1 Використання тестування для випробувань апаратних засобів. 2 Використання тестування для випробувань пам'яті.	2 2

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
3 Використання тестування для випробувань на граничні навантаження.	2,3
4 Використання тестування для випробувань на беззбійність.	2,3
5 Використання тестування для випробувань на відновлюваність.	2,3
6 Використання тестування для випробувань системи ТЗІ.	2
7 Використання тестування для випробувань продуктивності (навантажувальної спроможності).	2
8 Використання тестування для випробувань на надійність, готовність і відмовостійкість.	2,3
9 Використання тестування для випробувань засобів взаємодії з користувачем.	2
Ф02/МОН\ЗВ\ПЗ’ТЗ\Ш Ф04/МОН\ПЗ’ТЗ\ЗВ\ЕУ Ф05/МОН\ПЗ’ТЗ\ЗВ\ПЦ Ф06/МОН\ПЗ’ТЗ\ЗК/ІС	
1 Програмно-логічний контроль конфігурації і цілісності програмно-технічних засобів АТС.	2
2 Апаратний контроль конфігурації і цілісності програмно-технічних засобів АТС.	3
Ф02/ПТД/Г/ТЗ\НК\АЛ\Ц\Ш	
1 Використання групових засобів протидії з боку станційного устаткування несанкціонованому користуванню цифровими абонентськими лініями, що базуються на циклічному і (або) програмно-керованому моніторингу позаштатних змін електричних параметрів цифрових абонентських ліній.	3
Ф02/ПТД/Г/ТЗ\НК\АЛ\А\Ш	
1 Використання групових засобів протидії з боку станційного устаткування несанкціонованому користуванню цифровими абонентськими лініями, що базуються на циклічному і (або) програмно-керованому моніторингу позаштатних змін електричних параметрів аналогових абонентських ліній.	3
Ф03/ВЯВ\ЕП	
1 Установка технічних засобів виявлення і реєстрації відхилень параметрів енергопостачання АТС.	1
Ф03/НТР\ЕП	
1 Нейтралізація змін параметрів живлячої напруги за допомогою пристроїв, що фільтрують і стабілізують.	2
2 Нейтралізація змін параметрів живлячої напруги шляхом переключення на резервне джерело живлення.	3
Ф03/ВЯВ\ЕМ	
1 Установка технічних засобів виявлення і реєстрації підвищення рівня електромагнітних випромінювань (ЕМВ).	1
Ф03/НТР\ЕМ	
1 Нейтралізація впливу ЕМВ шляхом екранування критичних елементів устаткування.	2
2 Застосування схемотехнічних рішень, що виключають можливість впливу ЕМВ на роботу АТС	3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф03/ВЯВ\УФ	
1 Установка технічних засобів виявлення і реєстрації ультрафіолетового випромінювання (УФВ)	1
Ф03/НТР\УФ	
1 Застосування засобів або конструктивних заходів, що обмежують влучення УФВ на критичні елементи (наклейки-пломби, фарби, лаки, монтаж мікросхем постійної пам'яті з ультрафіолетовим стиранням «вікном» вниз і т. ін.). 2 Застосування елементів, некритичних до впливу УФВ	2 3
Ф03/ПВІ/ЗЗ\НМ\ЕУ	
1 Установка захисних пристроїв у лініях зв'язку, живлення і інших критичних елементів устаткування	2
Ф03/ОХР\ТЗ Ф12/ОХР\ТЗ'ФН	
1 Застосування надійної упаковки. 2 Використання захисних покрить. 3 Застосування віброгасників	1 1 1
Ф03/НТР\ЗВ\СЩ\ПЗ'ТЗ	
1 Використання засобів активної нейтралізації джерел негативних впливів на елементи АТС	2,3
Ф03/ПТР\ТР	
1 Підтримка оптимальної температури навколишнього середовища АТС за допомогою кондиціонування, примусової вентиляції і т. ін.	1,2,3
Ф04/МСК\ОД\ЗВ\ЕУ Ф05/МСК\ОД\ЗВ\ПЦ Ф06/МСК\ОД\ЗК	
1 Застосування програмно-технічних засобів генерації маскуючих сигналів	2,3
Ф04/ПТД/ТЗ/О\НК\АЛ\А	
1 Застосування індивідуальних засобів протидії несанкціонованому користуванню аналоговою абонентською лінією АТС, які базуються на виявленні і придушенні технічними засобами захисту тих сигналів, що ініціюються позаштатними прикінцевими пристроями в процесі взаємодії зі станційними абонентськими комплектами	1
Ф04/КЕР\ЗН\ЗВ\ЕУ	
1 Наявність засобів керування засобами нейтралізації позаштатних впливів на елементи устаткування АТС	1
Ф04/ВЯВ/ПЗ'ТЗ/О\НК\АЛ\А Ф06/МНЛ\ЗК	
1 Застосування технічних засобів виявлення змін електричних параметрів лінії при підключенні нештатних кінцевих пристроїв. 2 Використання засобів нелінійної локації нештатних кінцевих пристроїв	1,2 2
Ф04/ЗНЩ\ЗВ Ф05/ЗНЩ\ЗВ Ф06/ЗНЩ\ЗК'СГ	
1 Знищення джерел загроз для інформаційних ресурсів АТС на логічному рівні.	1

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
2 Знищення джерел загроз для інформаційних ресурсів АТС на програмно- апаратному рівні.	2
3 Знищення джерел загроз для інформаційних ресурсів АТС на фізичному рівні	3
Ф04/РДО\ПЦ\ЗВ\ЕУ Ф05/РДО\ПЦ\ЗВ Ф06/РДО\ПЦ/ЗК Ф11/РДО\ФН	
1 Реалізується протокол однопрохідної сильної ідентифікації й автентифікації під час входу в систему за допомогою атестованих прграмно-технічних засобів із використанням паролю умовно-постійної дії довжиною не менше ніж вісім літеро-цифрових символів.	1,2
2 Забезпечується підтримка нерозривного зв'язку унікального ідентифікатора користувача (в тому числі, осіб із складу персоналу АТС) з усіма його діями.	1,2,3
3 Реалізується механізм захисту даних автентифікації від будь-яких неуповноважених суб'єктів доступу, включаючи персонал АТС.	1,2,3
4 Реалізуються механізми контролю правил домінування повноважень користувача над рівнями і повноваженнями створюваних ним суб'єктів (програм, процесів та ін.).	1,2,3
5 Реалізується ідентифікація програм, томів, каталогів, файлів, записів, полів записів і інших логічних об'єктів доступу за іменами.	1,2
6 Реалізується ідентифікація терміналів, прикінцевих пристроїв, процесорів, каналів зв'язку і інших фізичних об'єктів доступу за логічними іменами і (або) адресами.	1
7 Реалізується ідентифікація терміналів, прикінцевих пристроїв, процесорів, каналів зв'язку і інших об'єктів доступу за фізичними адресами (номерами).	2
8 Реалізується підтримка виділеного захищеного каналу між користувачами АТС (в тому числі, осіб із складу персонала АТС) і базою захисту АТС, зв'язок через який може ініціюватись тільки користувачем.	2
9 Реалізується протокол багатопрохідної сильної автентифікації за допомогою атестованих програмно-технічних засобів.	3
10 Реалізується апаратна ідентифікація і перевірка істинності терміналів, прикінцевих пристроїв, процесорів, каналів зв'язку і інших об'єктів доступу до унікальних вмонтованих пристроїв.	3
11 Здійснюється ідентифікація і перевірка істинності програм, томів, каталогів, файлів, записів, полів записів за іменами і контрольними сумами (паролями, ключами).	3
12 Здійснюється керування потоками інформації на АТС за допомогою міток конфіденційності; при цьому дозволений рівень доступу до нагромаджувачів повинен бути не нижче дозволених рівнів доступу до інформації, яка на них записується.	3
13 Реалізується підтримка виділеного захищеного каналу між користувачем АТС (включаючи осіб із складу персонала АТС) і базою захисту АТС, зв'язок через який може ініціюватися як з боку користувача, так і з боку бази захисту.	3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
14 Реєстрація користувачів під час входу в середовище АТС повинна здійснюватися з використанням атестованих ідентифікованих фізичних пристроїв (жетонів, магнітних карт, електронних ключів і т. ін.) або пристроїв автентифікації за біометричними характеристиками	3
Ф04/ПТД/Г/ЕУ\НК\АЛ\А	
1 Використання засобів, заснованих на циклічному і (або) програмно-керованому моніторінгу нештатних змін електричних параметрів абонентських ліній	2,3
Ф05/ІЗЛ\СЗ/ПЗ	
1 Логічна ізоляція модулів системного програмного забезпечення. 2 Програмна ізоляція модулів системного програмного забезпечення. 3 Апаратна ізоляція модулів системного програмного забезпечення	1 2 3
Ф05/КЕР\ЗЗ’ЗН\ЗВ\ПЦ	
1 Наявність засобів керування засобами нейтралізації позаштатних впливів на програми, дані і процеси на АТС	2,3
Ф05/КТР\КФ’ЦЛ\ПЗ’ТЗ Ф06/КТР\КФ’ЦЛ\ПЗ’ТЗ Ф05/КТР\ЦЛ\ЗЗ\ЗВ\ПЦ Ф06/КТР\ЦЛ\ЗЗ\ЗК/ПЗ’ТЗ Ф06/КТР\КФ/ПЗ’ТЗ\ЗК	
1 Використання вбудованих процедур тестування. 2 Використання методів, заснованих на введенні апаратної надмірності. 3 Реалізація програмно-апаратних засобів безперервного контролю конфігурації і цілісності програмно-технічних засобів АТС	1 2 3
Ф06/ВЯВ\ЗК/ІС Ф06/ВЯВ\ЗК/МА	
1 Використання засобів постійної реєстрації параметрів системи, що дозволяють виявити спроби активізації закладних пристроїв і зафіксувати моменти їх активізації	2,3
Ф06/ПТР/ЗН\ЗК	
1 Наявність засобів керування засобами нейтралізації закладних пристроїв	2,3
Ф06/КТР/ЕЛ\ЗК\ЕУ	
1 Використання технічних пристроїв для спостереження за електричними параметрами контрольованих частин устаткування АТС	2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф07/ВЯВ\ПЕ\МЗ; Ф07/ВЯВ\ПЕ/І\МЗ; Ф07/РЕС\ПЕ\МЗ; Ф07/РЕС\ПЕ/І\МЗ; Ф07/МОН\ПЕ\МЗ; Ф07/МОН\ПЕ/І\МЗ; Ф07/ОСЛ\ПЕ\МЗ; Ф07/ОСЛ\ПЕ\І\МЗ; Ф07/МСК\ПЕ\МЗ; Ф07/МСК\ПЕ/І\МЗ; Ф07/ВЯВ\НД/АЛ/Ц; Ф07/ВЯВ\НД/АЛ/А; Ф07/ВЯВ\НД/І/ЕМ/СГ/АЛ/А; Ф07/ВЯВ\НД/І/ЕМ/СГ/АЛ/Ц; Ф07/РЕС\НД/АЛ/Ц; Ф07/РЕС\НД/АЛ/А; Ф07/РЕС\НД/І/ЕМ/СГ/АЛ/А; Ф07/РЕС\НД/І/ЕМ/СГ/АЛ/Ц; Ф07/МОН\НД/АЛ/Ц; Ф07/МОН\НД\АЛ/А; Ф07/МОН\НД/І/ЕМ/СГ/АЛ/А; Ф07/МОН\НД/І/ЕМ/СГ/АЛ/Ц; Ф07/ОСЛ\НД/АЛ/Ц; Ф07/ОСЛ\НД/АЛ/А;Ф07/ОСЛ\НД/І/ЕМ/СГ/АЛ/А; Ф07/ОСЛ\НД/І/ЕМ/СГ/АЛ/Ц; Ф07/МСК\НД/АЛ/Ц; Ф07/МСК\НД/АЛ/А; Ф07/МСК\НД/І/ЕМ/СГ/АЛ/А; Ф07/МСК\НД/І/ЕМ/СГ/АЛ/Ц; Ф07/ВЯВ\НД\ТЛ; Ф07/ВЯВ\НД\ЛУ; Ф07/ВЯВ\НД\МЛ; Ф07/ВЯВ\НД\ЛК\ЗХ; Ф07/РЕС\НД\ТЛ; Ф07/РЕС\НД\ЛУ; Ф07/РЕС\НД\МЛ; Ф07/РЕС\НД\ЛК\ЗХ; Ф07/МОН\НД\ТЛ; Ф07/МОН\НД\ЛУ; Ф07/МОН\НД\МЛ; Ф07/МОН\НД\ЛК\ЗХ; Ф07/ОСЛ\НД\ТЛ; Ф07/ОСЛ\НД\ЛУ; Ф07/ОСЛ\НД\МЛ; Ф07/ОСЛ\НД\ЛК\ЗХ; Ф07/МСК\НД\ТЛ; Ф07/МСК\НД\ЛУ; Ф07/МСК\НД\МЛ; Ф07/МСК\НД\ЛК\ЗХ; Ф08/ВЯВ\АЕ\АЛ\А; Ф08/ВЯВ\АЕ\ТЛ\СК; Ф08/ВЯВ\СГ/ВЧ\АЛ\Ц; Ф08/ВЯВ\СГ/ВЧ\АЛ\А; Ф08/ВЯВ\СГ/ВЧ\ТЛ\СК; Ф08/ВЯВ\ВМ/ВЧ\ЕМ; Ф08/РЕС\АЕ\АЛ\А; Ф08/РЕС\АЕ\ТЛ\СК; Ф08/РЕС\СГ/ВЧ\АЛ\Ц; Ф08/РЕС\СГ/ВЧ\АЛ\А; Ф08/РЕС\АЕ/І/Ц\АЛ\А; Ф08/РЕС\СГ/ВЧ\ТЛ\СК; Ф08/РЕС\ВМ/ВЧ\ЕМ; Ф08/МОН\АЕ\АЛ\А; Ф08/МОН\АЕ\ТЛ\СК; Ф08/МОН\СГ/ВЧ\АЛ\Ц; Ф08/МОН\СГ/ВЧ\АЛ\А; Ф08/МОН\СГ/ВЧ\ТЛ\СК; Ф08/МОН\АЕ/І/А\АЛ\Ц; Ф08/МОН\ВМ/ВЧ\ЕМ; Ф08/ОСЛ\АЕ\АЛ\А; Ф08/ОСЛ\АЕ\ТЛ\СК; Ф08/ОСЛ\СГ/ВЧ\АЛ\Ц; Ф08/ОСЛ\СГ/ВЧ\АЛ\А; Ф08/ОСЛ\СГ/ВЧ\ТЛ\СК; Ф08/ОСЛ\ВМ/ВЧ\ЕМ; Ф08/МСК\АЕ\АЛ\А; Ф08/МСК\АЕ\ТЛ\СК; Ф08/МСК\СГ/ВЧ\АЛ\Ц; Ф08/МСК\СГ/ВЧ\АЛ\А; Ф08/МСК\СГ\ТЛ/ВЧ\СК; Ф08/МСК\ВМ/ВЧ\ЕМ; Ф09/НТР\КВ\ІУ; Ф09/КТР\ЦЛ\ЗЗ\ІУ; Ф09/ВЯВ\МА\ІУ; Ф09/ПТД\НК\РР/ІУ	
1 Рівні стійкості механізмів захисту вищеназваних ФПЗ у цьому НД не специфікуються. Специфікації цих механізмів захисту визначаються за допомогою окремих спеціалізованих методик, що узгоджуються з уповноваженим державним органом	1,2,3
Ф10/ЗРЧ\СК	
1 Наявність інтерфейсу користувачів типу «меню» і т. ін.	1
2 Наявність вмонтованих контекстно-залежних підказок.	1
3 Наявність можливостей роботи з «гарячими» клавішами.	1
4 Можливість використання макрокоманд.	1
5 Можливість роботи з групами даних.	1
6 Багатократне підтвердження «небезпечних» команд.	2
7 Наявність перевірки на допустимість команд у конкретних ситуаціях.	2
8 Застосування параметрів за умовчанням, що забезпечують нормальну роботу АТС.	2
9 Забезпечення підтвердження проходження команд через систему.	1
10 Застосування термінів та скорочень на мові користувача.	1
11 Можливість завдання параметрів команд на електронному бланку.	1
12 Інтуїтивно-зрозумілий інтерфейс.	1

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
13 Відображення динаміки виконання команд.	1
14 Забезпечення зручного доступу до елементів технічних засобів АТС (типових елементів заміни, кабелів, роз'єднувачів і т. ін.).	1
15 Наявність схем послідовностей дій персоналу для наперед передбачуваних ситуацій.	1
16 Наявність схем робочих станів АТС і переходів між ними	1
Ф10/ЗРЧ\АЛ	
1 Забезпечення індикації на дисплеї абонента сервісної інформації.	1
2 Забезпечення можливості роботи як з імпульсним, так і з тональним набором номера.	2
3 Забезпечення можливості одержання абонентом оперативних довідок про режими і функції АТС.	2
4 Забезпечення можливості заборони з'єднань визначеним користувачам.	1
5 Реалізація базового набору сервісних функцій і послуг станції	2
Ф10/ЗМН\ЗБ	
1 Вибір надійної елементної бази (в т.ч., за рахунок відбракування, тренування і випробування елементів).	1,2
2 Раціональне компонування і дотримання правил монтажу.	1
3 Екранування пристроїв, що прийнятні до завад.	1
4 Установка розв'язуючих і подавляючих фільтрів у ланцюгах живлення.	1,2
5 Використання гальванічно-розв'язаних ланцюгів із симетричними входами і виходами.	1,2
6 Використання ліній зв'язку, не чуттєвих до зовнішніх наводів.	2
7 Вибір полегшених електричних і теплових режимів роботи елементів.	1
8 Використання стандартизації й уніфікації елементів і пристроїв.	1
9 Застосування системи контролю якості.	1
10 Створення схем з обмеженими наслідками відмов елементів.	1,2
11 Використання раціональних методів профілактичних заходів.	1
12 Використання обмеження навантаження елементів устаткування.	1
13 Використання заводських випробовувань.	2
14 Використання приймально-здавальних випробовувань	2
Ф10/НМР/С/ТЗ	
1 Використання «зчетвереної» логіки з переплетеннями.	2
2 Використання інших способів введення структурної надмірності	1,2,3
Ф10/НМР/І/ПЗ	
1 Використання кодів із виявленням і виправленням помилок.	1,2,3
2 Використання розподілу бітів пам'яті даних між мікросхемами пам'яті для можливості корекції даних у разі відмови однієї з мікросхем.	2
3 Використання інших способів введення інформаційної кодової надмірності	1,2,3
Ф10/НМР/СГ/ТЗ'ПЗ	
1 Використання методів кодування/декодування сигналів.	1,2
2 Використання багатопозиційних методів модуляції/демодуляції сигналів.	2
3 Використання інших способів введення сигнальної надмірності	1,2,3

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф10/НМР/ТЗ/А	
1 Використання алгоритмічної надмірності апаратних засобів для виявлення і вилучення наслідків збоїв і відмов у роботі устаткування	2
Ф10/НМР/ПЗ'Ф	
1 Використання функціональної надмірності. 2 Використання програмної надмірності	2 2
Ф10/НМР/ПЗ/А	
1 Використання «нечутливих» (до виникнення помилок) алгоритмів. 2 Використання інших методів алгоритмічної надмірності	2,3 1,2,3
Ф10/НМР/ПЗ/С	
1 Використання методу контрольних функцій. 2 Використання надмірності операційного середовища (наприклад, принципу віртуальних машин, концепції монітора і т. ін.). 3 Використання інших методів структурної надмірності програмного забезпечення	1,2 2,3 1,2,3
Ф10/ВКР/ПЗ/Д	
1 Використання доказових методів програмування	2
Ф10/ВКР/ПЗ/С	
1 Використання структурних методів розробки програмного забезпечення і структурування масивів даних	2
Ф10/ВКР/ПЗ/М	
1 Створення модульного програмного забезпечення	2,3
Ф10/ТСТ\ПЗ/С	
1 Використання статичних тестів. 2 Використання динамічних тестів (тобто, коли тестують усі логічні гілки програм). 3 Використання верифікації програмного забезпечення. 4 Використання символічного тестування за допомогою тестових наборів. 5 Використання генерації структурних тестів. 6 Використання інших структурних методів тестування програмного забезпечення	1 2,3 2 2 2 2,3
Ф10/ПТД\ПЗ\Щ	
1 Реалізація захисту від можливості завантаження позаштатного програмного забезпечення	1
Ф10/ПТД\ТЗ\ЗК	
1 Реалізація конструктивних елементів АТС, що затруднюють можливість установки закладних пристроїв	1
Ф10/ПТД\М/РЕ\ЕУ	
1 Застосування механічних засобів, що обмежують фізичний доступ до елементів устаткування АТС	1
Ф10/ВЯВ\НК\ЕУ	
1 Виявлення і реєстрація спроб несанкціонованого доступу до елементів устаткування	1
Ф11/КТР\ЦЛ\ПЗ	
1 Підтримка програмних засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів.	1

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
2 Підтримка програмно-технічних засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів.	2
3 Підтримка технічних засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів	3
Ф11/КТР\ЦЛ\ЗЗ	
1 Підтримка програмних засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів бази захисту.	1
2 Підтримка програмно-технічних засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів бази захисту.	2
3 Підтримка технічних засобів перевірки автентичності (цілісності) еталонних копій об'єктних модулів бази захисту	3
Ф11/КТР\ФН	
1 Реєстрація спроб доступу суб′єктів до фізичних носіїв.	1
2 Підтримка атрибутів максимального і мінімального рівнів доступу.	2,3
3 Використання резервних копій інформаційних ресурсів, що містяться на фізичних носіях	3
Ф12/РЕЗ/ТЗ	
1 Дублювання елементів на різних структурних рівнях устаткування АТС.	2,3
2 Троювання елементів устаткування з мажоритарною вирішальною схемою.	3
3 Холодне резервування контуру керування АТС.	2
4 Холодне резервування абонентських комплектів.	2
5 Холодне резервування цифрового комутаційного поля.	2
6 Холодне повне загальне резервування АТС.	2
7 Холодне повне роздільне (поблочне) резервування.	3
8 Гаряче резервування контуру керування.	2
9 Гаряче резервування абонентських комплектів.	2
10 Гаряче резервування цифрового комутаційного поля.	2
11 Гаряче повне загальне резервування.	3
12 Гаряче повне роздільне (поблочне) резервування.	2
13 Використання інших методів апаратного резервування	2,3
Ф12/НМР/ТЗ/Т	
1 Використання функціональної інерційності суміжних пристроїв, що входять у АТС, для одержання тимчасової надмірності.	1,2
2 Використання специфічних умов взаємодії пристроїв, що входять у АТС, для одержання тимчасової надмірності.	1,2
3 Використання запасу продуктивності для одержання тимчасової надмірності.	2
4 Комплексування пристроїв однакового призначення для одержання тимчасової надмірності.	1,2
5 Використання особливостей у способах завантажування підсистеми АТС завданнями (заявками), у тому числі концентрування навантаження для одержання тимчасової надмірності.	2
6 Використання аварійного перезавантаження системи із захистом напівпостійних і оперативних даних.	1,2
7 Використання інших методів одержання тимчасової надмірності	1,2

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф12/НОВ\ЗЗ\РР\І	
1 Використання дуального або N-версійного програмування.	3
2 Використання резервної копії програмного забезпечення на зовнішньому носії.	2
3 Використання інших методів алгоритмічного і (або) технологічного резервування програм	2,3
Ф12/ВКР/ЕУ/З	
1 Використання резерву у виді комплекту запасного устаткування	1
Ф12/КТР\ПЗ’ТЗ	
1 Використання оперативного контролю за модулем.	2
2 Використання кодового контролю (за виявленням і виправленню помилок).	2,3
3 Використання контролю дублюванням або троюванням роботи пристроїв АТС.	2,3
4 Використання параметричного контролю.	2
5 Використання контролю справності абонентських ліній.	2
6 Використання інших методів апаратного оперативного контролю	2,3
Ф12/КТР\ПЗ	
1 Використання контролю тривалості виконання програм.	2,3
2 Використання контролю послідовності виконання програм.	2
3 Використання контролю «гладкості» результатів.	1,2
4 Використання методу контрольних функцій.	2
5 Використання контролю методом зворотного перетворення результатів.	2
6 Використання контролю шляхом логічного порівняння результатів роботи функціонально однакових модулів.	3
7 Використання контролю з використанням механізмів внесення алгоритмічної, програмної або тимчасової надмірності.	2
8 Використання детермінованого тестування за змістовними ознаками.	2
9 Використання логічного тестування для контролю комбінаційних схем без пам’яті.	2
10 Використання інших способів програмно-логічного контролю	1,2,3
Ф12/ЗМН\ТВ\ПЗ’ТЗ	
1 Використання захисту напівпостійних і оперативних даних у випадку аварійних перезавантажень програмного забезпечення.	2
2 Використання тимчасового резервування і інших раціональних способів експлуатації з метою зменшення середнього часу відновлення.	2
3 Використання засобів контролю і діагностування (в т.ч., вмонтованого) для зменшення середнього часу відновлення.	1
4 Використання контролеспроможних технічних засобів, які можуть бути відновленими	1
Ф12/КТР\МВ	
1 Використання обслуговуючого (сервісного) процесора для діагностування з жорстким ядром.	3
2 Використання взаємного діагностування в системах із розподіленим плаваючим ядром.	3
3 Використання взаємного діагностування в системах із розподіленим плаваючим ядром.	2

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф12/РКФ\НТР\ЗБ	
1 Використання автоматичної реконфігурації програмно-технічних засобів АТС після виявлення і локалізації несправності за рахунок «витрат» структурної надмірності системи.	3
2 Використання автоматичної реконфігурації програмно-технічних засобів АТС після виявлення і локалізації несправності за рахунок «витрат» функціональної надмірності системи.	3
3 Використання автоматичної реконфігурації програмно-технічних засобів АТС після виявлення і локалізації несправності за рахунок «витрат» сигнальної надмірності системи.	3
4 Використання реконфігурації програмно-технічних засобів АТС за рахунок спрощення структури використання «полегшених» режимів після виявлення і локалізації несправності.	2
5 Використання методу відступу («відкату»), тобто скороченого обслуговування після виявлення і локалізації несправності.	2
6 Використання інших методів введення динамічної надмірності в програмне забезпечення АТС.	2,3
7 Введення багатопроцесорності і організації спеціальних каналів зв'язку між процесорами (тобто, використання принципу розподіленого керування) для обміну в реальному часі службовою інформацією, необхідною для автоматичної реконфігурації системи у випадку відмов її елементів	2,3
Ф12/ІЗЛ\ЗБ	
1 Використання методів виключення впливу елементів, що відмовили, на нормальну роботу АТС.	2
2 Використання методів ізоляції помилок	2
Ф12/РДЛ\РР\Т'П	
1 Використання просторового рознесення елементів, що резервуються.	3
2 Використання рознесення у часі елементів, що резервуються.	2
3 Використання частотного (спектрального) рознесення елементів, що резервуються.	1
4 Використання кодового рознесення елементів, що резервуються	1
Ф12/ОРГ\ВС/ФЕ	
1 Використання елементів однакового функціонального призначення, але заснованих на різній фізичній природі функціонування	2,3
Ф12/НТР\НП\ПЗ'ТЗ	
1 Використання засобів активної нейтралізації джерел негативних впливів на програмно-технічні засоби АТС після їхнього виявлення і локалізації	2,3
Ф12/ТСТ/П\НВ\ЗХ	
1 Використання монолітних нерозбірних компонент устаткування, що самознищують свою структуру при спробі несанкціонованого доступу	2,3
Ф12/АНЛ\ЗБ	
1 Накопичення, зберігання та аналіз інформації про збої та відмови	2

Закінчення таблиці 7

Ознака механізму, що реалізує ФПЗ	Рівень стійкості
Ф12/ОРГ\ТО	
1 Можливість технічного обслуговування та ремонту устаткування за допомогою виробника АТС.	2,3
2 Можливість технічного обслуговування та ремонту устаткування компанією, яка спеціалізується на експлуатації АТС.	2,3
3 Можливість доробки, модернізації та актуалізації устаткування за допомогою виробника АТС	2,3