НОРМАТИВНИЙ ДОКУМЕНТ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Технічний захист інформації
на програмно-керованих АТС загального користування

Методика оцінки захищеності інформації
(базова)

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

Методика оцінки захищеності інформації

(базова)

НД ТЗІ 3.7-002-99

ДСТСЗІ СБ України

Київ

Зміст

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

НА ПРОГРАМНО-КЕРОВАНИХ АТС ЗАГАЛЬНОГО КОРИСТУВАННЯ

ОСНОВНІ ПОЛОЖЕННЯ

Чинний від 1999-07-01

1 Галузь використання

Цей нормативний документ (НД) містить основну (базову) методику оцінки захищеності інформації, що циркулює на програмно-керованих АТС загального користування, а також на установських (відомчих, корпоративних) АТС.

Положення НД поширюються на програмно-керовані АТС (далі - АТС), у яких зберігається та циркулює інформація, що підлягає технічному захисту (див. ДСТУ 3396.0 і НД ТЗІ 1.1-001-99).

Методика, яка викладена у НД, може бути реалізована, якщо відома модель загроз інформаційним ресурсам оцінюваної АТС.

Вимоги НД не поширюються на захист:

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

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

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

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

2 Нормативні посилання

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

- ДСТУ 2615-94 - Електрозв'язок. Зв'язок цифровий та системи передачі цифрові. Терміни та визначення;
- ДСТУ 2621-94 - Зв'язок телефонний. Загальні поняття. Телефонні мережі. Терміни та визначення.
- ДСТУ 3396.0-96 - Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96 - Захист інформації. Технічний захист інформації. Порядок виконання робіт;
- ДСТУ 3396.2-97 - Захист інформації. Технічний захист інформації. Терміни і визначення;
- ДСТУ 3413-96 - Захист інформації. Технічний захист інформації. Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції;
- ГОСТ 2.106-96 - ЕСКД. Текстовые документы;
- НД ТЗІ 1.1-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення;
- НД ТЗІ 2.7-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт;
- НД ТЗІ 2.5-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;
- НД ТЗІ 2.5-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту;
- НД ТЗІ 2.5-003-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

3 Визначення, позначення і скорочення

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Механізм захисту - процедура або частина процедури реалізації певної ФПЗ.

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

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

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

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

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 захисту 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 порушника 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 оцінювальних робіт;

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

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

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

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

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

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

4 Загальні положення

4.1 Для одержання впевненості в тому, що АТС забезпечує очікувану якість захисту інформаційних ресурсів, необхідне підтвердження досягнутого рівня якості такого захисту з боку незалежного експерта.

4.2 Якщо метою оцінки є одержання формального юридично дієвого документа, що підтверджує досягнутий рівень захищеності АТС за ТЗІ, то за експерта повинна виступати незалежна від усіх зацікавлених у результатах оцінки сторін спеціалізована організація, що має відповідні повноваження (ліцензію) від державного органу, який регламентує діяльність в галузі ТЗІ.

4.3 Ініціатором проведення оціночних робіт, тобто Заявником, може бути будь-яка юридична або фізична особа незалежно від громадянства або місця реєстрації підприємства.

Як правило, в одержанні сертифіката з оцінкою якості ТЗІ на АТС зацікавлені Виробник і (або) Постачальник АТС, а в одержанні атестата - Споживач (Покупець, Одержувач, Власник, Оператор зв'язку і т.ін.) виробу, який планує розгорнути АТС на своїх площах і тому зацікавлений у безпечній її експлуатації.

У окремих випадках ініціатором проведення оціночних робіт може бути організація (наприклад, комерційна, науково-дослідна, конструкторська, експертно-аналітична, державного керування і т.ін.), що зацікавлена в об'єктивних оцінках рівня захищеності інформаційних ресурсів на досліджуваній АТС.

4.4 Нормативна база України в галузі ТЗІ гармонізована (погоджена у методологічному плані) із Єдиними (уніфікованими) для Європейського Союзу критеріями оцінки безпеки систем інформаційної техніки (ITSEC). Оскільки програмно-керовані АТС належать до класу систем інформаційної техніки, то методика оцінки захищеності інформації на них повною мірою визначається вищезгаданими критеріями ITSEC із врахуванням специфічних особливостей АТС як інформаційно уразливого об'єкта.

4.5 Згідно цій методиці оцінка захищеності інформації на АТС проводиться в двох напрямках.

Перший напрямок містить у собі оцінку коректності (тобто, слушності) створеної на АТС системи ТЗІ, як-от:

- оцінюється коректність результатів проектування моделі захисту АТС, тобто визначається, чи дійсно запроектована множина ФПЗ з обраними в процесі проектування рівнями стійкості механізмів реалізації цих послуг може забезпечити необхідний рівень захисту інформаційних ресурсів від суттєвих для Заявника загроз;

- оцінюється коректність результатів проектування і реалізації КЗМЗ, тобто визначається, чи дійсно створений КЗМЗ безпомилково і повною мірою реалізує відображену у проекті множину ФПЗ;

- оцінюється ефективність системи ТЗІ на АТС , тобто визначається коректність результатів аналізу "слабких місць" у захисті інформаційних ресурсів з урахуванням особливостей конструкції АТС і умов її експлуатації.

Другий напрямок містить у собі оцінку рівня довіри до результатів, що отримані в процесі оціночних робіт у рамках першого напрямку, тобто оцінку рівня довіри до коректності реалізованої на АТС системи ТЗІ.

Тут мається на увазі, що висновок про коректність оцінюваної системи ТЗІ може бути зроблений на базі різної повноти і глибини знань про неї. Тому і рівень довіри до результатів оцінки коректності може бути різний.

Процес одержання довірчої оцінки полягає, в основному, у послідовному перегляді та перепровірці результатів і умов розробки, виготовлення, випробувань, поставки, введення в дію і експлуатації оцінюваної АТС на відповідність наданим у НД ТЗІ 2.5-003-99 довірчим критеріям.

4.6 Метою оцінки в рамках першого напрямку робіт є підтвердження слушності (безпомилковості, коректності) системи ТЗІ, що використовується на оцінюваній АТС.

Метою робіт, здійснюваних у рамках другого напрямку, є визначення ступеня впевненості (рівня довіри) у тому, що висновок про коректність реалізованої системи ТЗІ на АТС (отриманий, зокрема, як результат оціночних робіт за першим напрямком) є справедливим.

4.7 У випадку виявлення будь-яких некоректностей в оцінюваній системі ТЗІ на будь-якому із етапів її створення відпадає необхідність в оцінці рівня довіри до коректності, оскільки така коректність, відповідно до результатів оцінки, первісно відсутня.

4.8 Для оцінки коректності (слушності) моделі захисту така модель представляється Заявником у вигляді набору ФПЗ і відповідної множини реалізуючих ці ФПЗ механізмів захисту. Вказуються також мінімально припустимі рівні стійкості механізмів захисту.

У процесі оцінювання необхідно одержати підтвердження, що заявлена модель захисту належним чином протидіє саме тим загрозам, що є суттєвими для Заявника.

Не усі потенційно реалізовані на АТС загрози є суттєвими для її власників і користувачів, і не усякий ступінь протидії суттєвим загрозам із боку засобів і механізмів захисту їх може задовольнити. Можливі, наприклад, випадки, коли порушення конфіденційності інформації не спричиняють відчутних втрат для її власників. У цих випадках недоцільно витрачати ресурси на організацію захисту від такого виду загроз. Надмірний захист від суттєвих загроз може обумовити невиправдані витрати. Тому в процесі визначення необхідного рівня захищеності інформаційних ресурсів на АТС (див. НД ТЗІ 2.7 - 001 - 99) для кожної загрози, що віднесена до множини суттєвих загроз, указується гранично припустимий рівень втрат, які готовий

понести Заявник у разі реалізації такої загрози. А стійкість механізмів захисту, що протидіють цій загрозі, і ефективність системи захисту в цілому вибираються таким чином, щоб рівень витрат на створення захисних механізмів був менше або, у крайньому випадку, приблизно однаковим із гранично припустимим рівнем втрат, що пов'язані із можливою реалізацією такої загрози.

Аналіз домірності гранично припустимих втрат від можливих проявів загроз і запропонованих до реалізації рівнів стійкості механізмів захисту, що протидіють цим загрозам, і є предметом діяльності Експерта в процесі оцінки коректності моделі захисту.

Щодо цього проводиться перевірка функціональної повноти моделі (тобто, чи проти всіх суттєвих загроз організується захист), раціональності взаємозв'язків між ФПЗ і механізмами захисту в моделі (як-от, відсутність дублювання і надлишкового використання ресурсів, мінімізація витрат на захист і т.ін.). Перевіряється також спроможність функцій і механізмів захисту взаємодіяти таким чином, щоб взаємно підтримувати один одного і утворювати єдине діюче ціле.

4.9 Згідно з прийнятим у цьому документі підходом до оцінки захищеності АТС межа відповідальності Експерта починається з оцінки коректності моделі захисту. Отже, результати таких важливих етапів створення системи ТЗІ як аналіз середовища функціонування АТС з позицій ТЗІ (так званий аналіз чотирьох середовищ - інформаційного, користувачів, технологічного і середовища порушників), створення моделей порушників, побудова моделі загроз , аналіз ризиків і визначення необхідного рівня захищеності інформресурсів на АТС у процесі оціночних робіт на коректність не досліджуються.

Якщо Заявник не претендує на високі рівні довіри до коректності створеної системи ТЗІ, то для оцінки моделі захисту не потрібно надання результатів аналізу щодо середовищ функціонування АТС, моделей порушників та моделі загроз. Проте у міру підвищення претензій Заявника до рівня довірчих оцінок виникає необхідність у вивченні Експертом усе більш широкої номенклатури технічних документів, що відбивають усе більш глибоку й об'ємну роботу Заявника щодо рішення задач аналіза середовищ функціонування АТС, вибору моделі загроз, аналіза ризиків і визначення необхідного рівня захищеності АТС.

Щоб одержати високий рівень довіри до коректності моделі захисту, перераховані вище задачі мають вирішуватися напівформальними (у деяких випадках - формальними) шляхами із притягненням сучасних методів оптимального аналізу і синтезу структур.

4.10 Відповідальність за коректність визначення необхідного рівня захищеності інформаційних ресурсів на АТС покладається на Замовника і Розроблювача системи ТЗІ.

Для підтвердження високих рівнів довіри до коректності моделі захисту АТС із боку Експерта необхідно виконати ретельний аналіз усіх етапів розробки технічного завдання на створену систему ТЗІ для оцінюваної АТС.

4.11 Для оцінки коректності (слушності) КЗМЗ необхідно:

- оцінити функціональну повноту такого комплексу, тобто переконатися, що всі заявлені ФПЗ повною мірою реалізуються в оцінюваній системі;

- переконатися, що кожна з ФПЗ реалізується з рівнями стійкості механізмів захисту не меншими, ніж заявлені мінімально необхідні;

- переконатися, що існуючі на АТС механізми захисту відтворюють заявлені ФПЗ безпомилково - відповідно до нормуючих специфікацій цих послуг, що надані у НД ТЗІ 2.5-001-99.

Для оцінки коректності КЗМЗ Заявник у залежності від рівня довірчої оцінки передає Експертові документи з різним ступенем глибини і деталізації.

У випадках невисоких претензій на довіру щодо коректності досить перевірити документацію рівня користувачів. У цих випадках Експерт на підставі вивчення керівництв для користувачів і результатів "прогону" штатних функціональних тестів повинен переконатися, що є (або відсутні) зовнішні ознаки того, що в оцінюваній АТС дійсно реалізовані заявлені функції і механізми захисту.

У міру підвищення рівня довірчих оцінок відповідно підвищуються вимоги до ретельності і деталізації наданих для повторного огляду матеріалів. Зокрема, може виникнути необхідність у вивченні Експертом матеріалів робочого проектування - принципових схем технічних засобів, листінгів програм, спеціалізованих тестів і т.ін. Може також виникнути необхідність у проведенні додаткових випробувань з метою уточнення деталей функціонування того або іншого механізму захисту.

На високих рівнях довірчих оцінок у розпорядження Експерта повинна бути надана вичерпна інформація щодо техно-робочого проекту на систему ТЗІ для АТС і повна інформація про результати приймально-здавальних випробувань (зокрема, і за критеріями ТЗІ) із тим, щоб у нього склалося повне уявлення про роботу КЗМЗ.

4.12 У процесі оцінки коректності КЗМЗ необхідно підтвердити, що всі заявлені функції і механізми захисту реально діють на оцінюваній АТС відповідно до нормуючих специфікацій, що наведені в НД ТЗІ 2.5-001-99. Ступінь ретельності (досконалості) такого підтвердження залежить від претензій Заявника до рівня довіри, із яким треба ставитися до оцінки коректності КЗМЗ.

4.13 Розробка коректної моделі захисту, а також коректна реалізація ФПЗ і механізмів захисту в повній відповідності з нормуючими специфікаціями ще не гарантують досягнення необхідного рівня захищеності інформаційних ресурсів на АТС. У системі ТЗІ на АТС можуть бути , так звані "слабкі місця" або "виломи", через котрі або за допомогою яких можливі реалізації загроз для інформації.

Наприклад, функціонування певного засоба захисту через його якісну недосконалість може супроводжуватися утворенням побічного схованого каналу витоку. Становлять небезпеку різного роду побічні ефекти небажаної взаємодії функціонуючих засобів і механізмів захисту. Недосконалість конструкції елементів АТС, зокрема і засобів захисту, також може стати причиною загроз. Непередбачені можливості некоректного використання

програмно-технічних засобів АТС внаслідок порушень правил їхньої експлуатації, недосконалість прийомів експлуатації теж треба віднести до "слабких місць" системи ТЗІ. Особливо небезпечні з позицій захисту інформації потенційно можливі шляхи (прийоми, способи) обходу, обману, зміни, відключення, блокування реалізованих на АТС механізмів захисту. Тому аналіз "слабких місць" є необхідним елементом оцінки коректності КЗМЗ.

4.14 Якщо система ТЗІ на АТС забезпечує потрібні рівні стійкості до впливу прямих атак на використані механізми захисту, то ефективність такої системи захисту цілком залежить від рівня її досконалості стосовно слабких місць. Тому оцінка слабких місць у цьому документі називається оцінкою ефективності системи захисту.

4.15 Як правило, Заявник надає Експерту відомість (перелік) відомих "слабких місць" у проекті системи ТЗІ (на рівні як технічного, так і робочого проектування), а у випадку оцінки АТС у конкретних умовах експлуатації відомість, що відображає всі відомі Заявнику слабкі місця в експлуатації АТС. У цих відомостях повинно враховуватися кожне "слабке місце", міститися опис шляхів його створення і наслідків його можливого прояву, показуватися заходи щодо нейтралізації або зменшення негативних наслідків такого прояву. У необхідних випадках повинно бути надане пояснення (доказ), чому аналізоване "слабке місце" не впливає на політику безпеки на АТС , або чому воно не може проявитися в даних конкретних умовах експлуатації.

Повнота і ретельність аналізу "слабких місць", що представляється, повинна збільшуватися в міру жорсткості вимог до довірчої оцінки.

Якщо у випадках невисоких вимог до рівня довіри вимагаються обгрунтовані пояснення щодо "слабких місць", то на вищих довірчих оцінках необхідно представити напівформальні або формальні докази відсутності негативного впливу "слабких місць" на захищеність інформаційних ресурсів АТС.

4.16 Експерт переглядає отримані від Заявника матеріали щодо аналізу "слабких місць", намагаючись виявити як некоректності в наданих обгрунтуваннях, так і невраховані "слабкі місця" або "виломи" в захисті.

4.17 Оціночні роботи, що описані в 4.8 - 4.16, пов'язані з переглядом слушності побудови і реалізації системи ТЗІ на АТС .

Передбачається, що якщо система ТЗІ коректна, то вона і дієва в тому розумінні, що найбільш раціональним шляхом забезпечує необхідний Заявникові рівень захищеності інформаційних ресурсів (не більше і не менше). Тому нормуючі умови, вимоги і показники, згідно яких оцінюється коректність системи ТЗІ, у цьому документі називаються критеріями дієвості.

4.18 Для оцінки рівня довіри до коректності реалізації системи захисту використовуються довірчі критерії, що описані в НД ТЗІ 2.5-003-99.

У цьому документі специфікується сім можливих рівнів довіри (сім градацій в оцінці ступеня довіри) до коректності системи ТЗІ, як-от: рівні довіри ЕО, Е1, Е2, Е3, Е4, Е5 і Е6.

Найнижчий рівень довірчої оцінки - ЕО означає недостатню довіру до коректності системи ТЗІ в оцінюваній АТС. Рівень довіри Е1 є початковим рівнем, нижче якого раціональна довіра не зберігається. Рівень Е6 специфікує найвищий ступінь довіри. Інші рівні є проміжними.

4.19 Відповідно до прийнятого тут підходові до оцінки захищеності АТС при переході від більш низьких довірчих оцінок до більш високих вимоги до зростання кількості і (або) якості наданих на АТС функціональних послуг захисту не пред'являються, при цьому не пред'являються також вимоги до підвищення ступеня досконалості реалізованих у системі механізмів захисту. Тут прийнято вважати, що визначена у процесі проектування системи ТЗІ множина ФПЗ і створений у процесі реалізації проекту КЗМЗ або правильно (тобто, коректно) або неправильно (тобто, некоректно) підтримує необхідний рівень захищеності інформаційних ресурсів АТС, тобто є усього лише дві градації у визначенні коректності системи захисту - коректна або некоректна.

У той же час, якщо система захисту визнана коректною, то ступінь довіри до зробленого виводу про її коректність можливо відбити за допомогою семи градацій рівня довіри - від ЕО до Е6.

При цьому вимоги до глибини і широти аналізу умов створення і використання системи ТЗІ, до рівня формалізації і строгості доказів коректності побудованих моделей захисту, до старанності експериментальних досліджень коректності при переході до більш високих оціночних рівнів довіри, як це видно зі специфікацій рівнів довіри НД ТЗІ 2.5-003-99, істотно зростають.

4.20 У найпростішому випадку, коли Заявнику не потрібен високий рівень довіри до того, чи правильно спроектована і реалізована система захисту, то оціночні роботи можливо істотно спростити, узявши за вихідний матеріал для оцінки документацію на рівні керівництва користувача і не виконуючи в процесі оцінки складних і трудомістких робіт з аналізу і тестування механізмів захисту або аналізу загроз і "слабких місць" у захисті.

У іншому крайньому випадку, коли необхідно забезпечити найвищий рівень довіри до коректності оцінюваної системи ТЗІ на АТС , Заявник повинен представити Експерту поряд із документацією, що детально описує всі стадії життєвого циклу АТС (зокрема, середовище її створення й експлуатації) ще і серйозні тести "на проникнення" і вичерпний аналіз "слабких місць" у захисті, а також формальні докази коректності реалізованої на АТС технічної політики безпеки.

У реальному житті рівень довіри до коректності, що заявляється для оцінки, знаходиться десь посередині між описаними вище випадками.

4.21 Прийнята в цьому документі методика оцінки не припускає наявності однозначної залежності між вимогами до підтвердження коректності системи і рівня довіри до неї. Не всі комбінації функціональності і довіри можуть бути розумними або корисними. Наприклад, якщо АТС призначена для опрацювання секретної інформації і, тому, у ній реалізована якісна система ТЗІ з високою стійкістю механізмів захисту, то доцільно забезпечити високий рівень довіри до коректності такої системи.

З іншого боку, нерозумно вимагати високих довірчих оцінок до системи захисту, що побудована на базі механізмів з низькою стійкістю.

4.22 Для виконання оціночних робіт Заявник повинен надати Експерту можливість проведення спеціальних експериментальних досліджень програмних і технічних засобів оцінюваної АТС на розгорнутому працездатному зразку вироба (системи), а також штатні контрольно-вимірювальні і діагностичні засоби, необхідну технічну й організаційно-розпорядницьку документацію.

4.23 Зміст і обсяг здійснюваних у процесі оцінки експериментальних досліджень, перелік, зміст і форма необхідних для аналізу документів, рівень старанності (формалізації, деталізації) обгрунтувань і доказів, які надаються Заявником щодо різних аспектів реалізованої на АТС системи ТЗІ, однозначно залежать від заявленого рівня довіри до коректності системи захисту. Така залежність відображена у відповідних специфікаційних вимогах (див. НД ТЗІ 2.5 - 001 - 99, НД ТЗІ 2.5 - 002 - 99, НД ТЗІ 2.5 - 003 - 99).

4.24 Заявник несе повну відповідальність за працездатність наданого в розпорядження Експерта зразка виробу (системи), за працездатність і своєчасну перевірку штатних контрольно-вимірювальних і діагностичних засобів, за точність (слушність) наданої документації.

4.25 У цій методиці для кожного оціночного рівня визначені вимоги до переліку, змісту і формі документів, що повинний передати Заявник у розпорядження Експерта, і, отже, заздалегідь їх підготувати ще до проведення оціночних робіт.

4.26 У процесі оцінювання за вищими рівнями довіри (починаючи з рівня Е4) виникає необхідність у розробці і виготовленні спеціальних схем дослідження "слабких місць", глибоких тестів " на проникнення", моделювання дій "хакеров", формального опису політики безпеки. Всю вище перераховану роботу повинний узяти на себе Заявник і відповідати за повноту і коректність її виконання. Експерт може взяти на себе роботу з перегляду наданих Заявником тестів, моделей, схем, аналізів, обгрунтувань і доказів. Він має право їх доповнювати й удосконалювати, досліджувати власними методами і засобами слабкі місця в захисті.

4.27 Для всіх оціночних рівнів, за винятком Е1, Експерт повинен переважно перепровіряти результати випробувань і аналізу, які Заявник надав у його розпорядження.

4.28 На оціночному рівні Е1 оцінка може робитися тільки за результатами аналізу документації користувачів. Заявник у цьому випадку може і не надавати результати випробувань системи ТЗІ для АТС .

4.29 У процесі оціночних робіт може з'ясуватися, що який-небудь аспект оціночного рівня не виконується, наприклад через відсутність необхідної інформації або внаслідок того, що реальна характеристика оцінюваного об'єкта не відповідає нормуючим вимогам. У такому випадку Заявникові надається право в заздалегідь обумовлені терміни усунути зауваження (наприклад, дати відсутню інформацію, виправити помилку, доопрацювати елемент захисту і т.ін.). У протилежному випадку, оцінюваний об'єкт матиме результат оцінки за рівнем ЕО.

4.30. Для того, щоб оцінка була виконана ефективно і з мінімальними витратами, Експерт може співробітничати із Заявником і (або) Розроблювачем системи ТЗІ. Однак Експерт повинен бути незалежним у тому розумінні, що не брати участь у розробці системи ТЗІ для оцінюваної АТС.

5 Порядок виконання робіт з оцінки захищеності інформаційних ресурсів АТС

5.1 Для проведення оціночних робіт з оцінки захищеності інформаційних ресурсів АТС Заявник повинен підготувати і надати в розпорядження експертного органа відповідні заявочні документи.

5.2 Мета проведення оціночних робіт - підтвердити або спростувати зазначену в заявочних документах ступінь впевненості в тому, що система ТЗІ на оцінюваній програмно-керованій АТС коректно реалізована і забезпечує зазначений Заявником певний рівень захищеності інформаційних ресурсів.

5.3 Ступінь впевненості в коректності реалізованої системи ТЗІ, що відображається через заявлений до оцінки рівень довіри (один із шести можливих нормованих градацій - від Е1 до Е6), і рівень захищеності інформаційних ресурсів у вигляді певної множини ФПЗ з визначеними рівнями стійкості механізмів захисту, що реалізують ці послуги, вказуються Заявником в процесі оформлення заявки на виконання оціночних робіт, яка, в свою чергу, направляється на адресу уповноваженого державою органа з оцінки ТЗІ на цифрових комутаційних системах.

5.4 Розглянувши заявку, уповноважений орган надає Заявникові поштові реквізити експертів - незалежних від Заявника організацій (як правило, випробувальних лабораторій або центрів), що мають право і здатні виконувати роботи з оцінки захищеності інформаційних ресурсів АТС на очікуваному рівні довіри.

5.5 Заявник на власний розсуд вибирає Експерта із кола рекомендованих уповноваженим органом. Далі, відповідно до правил, які регламентовані в ДСТУ 3413-96 , укладається договір між Заявником, що виступає за Замовника, і Експертом, що виступає за Виконавця, на проведення оціночних робіт.

Результатом виконання оціночних робіт повинен бути висновок про те, чи дійсно система ТЗІ на оцінюваній АТС коректно забезпечує заявлений (очікуваний) рівень захищеності інформаційних ресурсів АТС, і у випадку підтвердження коректності системи захисту, чи дійсно ступінь довіри до висновку про коректність системи захисту знаходиться на рівні, що зазначив Заявник у заявочних документах.

5.6 Порядок виконання робіт показаний на рисунку 1.

5.7 Відповідно до цієї методики спочатку виконується оцінка коректності системи ТЗІ для оцінюваної АТС.

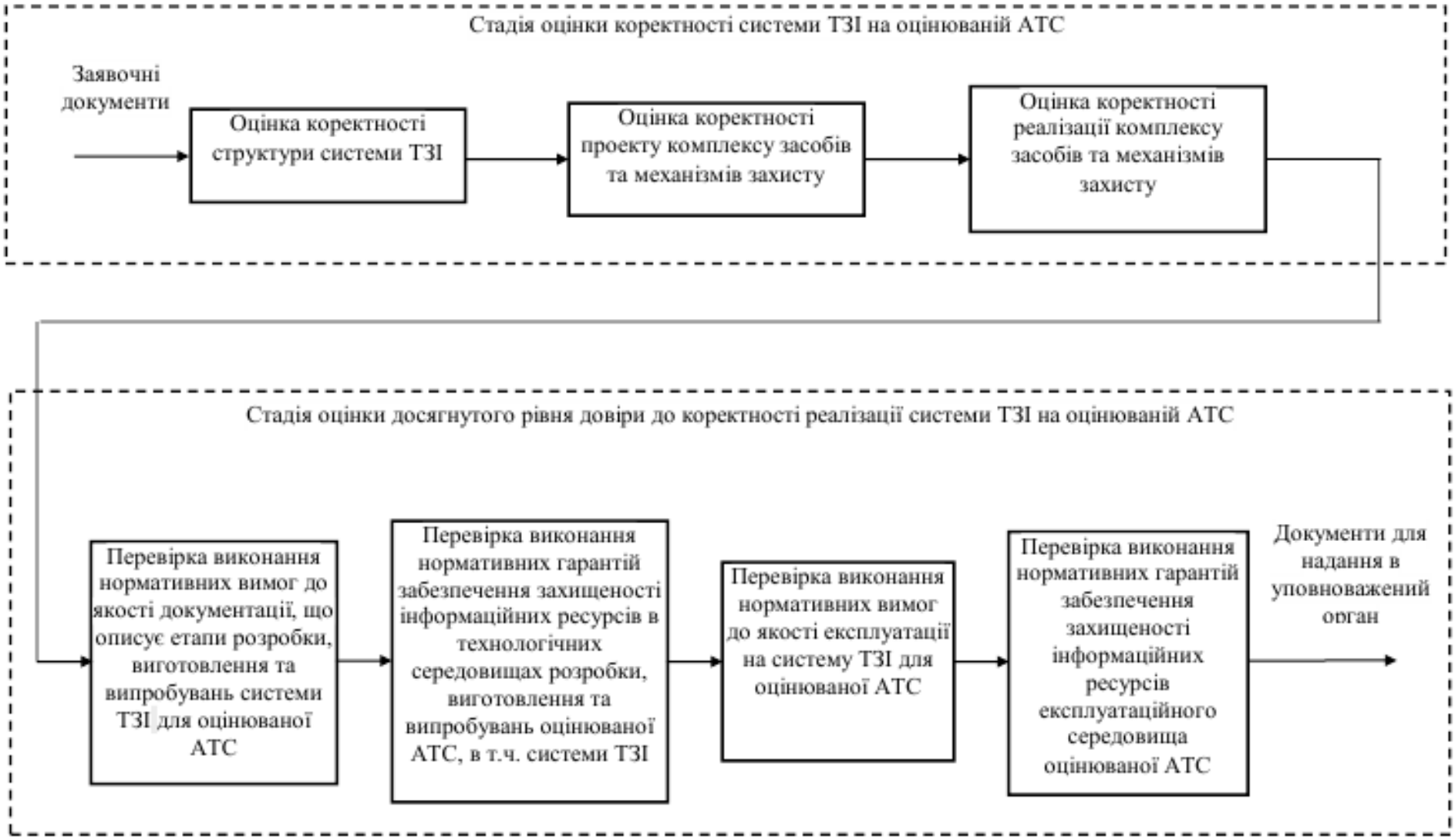

Рисунок 1 – Порядок виконання робіт з оцінки захищеності інформації на програмно-керованій АТС загального користування

Стадія оцінки коректності системи ТЗІ містить у собі послідовне виконання наступних видів робіт, названих далі опціями:

- оцінка коректності структури системи ТЗІ (опція 1.1);
- оцінка коректності проекта комплексу засобів і механізмів захисту (опція 1.2);
- оцінка коректності реалізації комплексу засобів і механізмів захисту (опція 1.3).

5.8 Зміст робіт за опцією 1.1 регламентований у розділі 6.1.

5.9 Зміст робіт за опцією 1.2 регламентований у розділі 6.2.

5.10 Зміст робіт за опцією 1.3 регламентований у розділі 6.3.

5.11 Порядок викладу матеріалів, що регламентують оцінку системи на відповідність критеріям дієвості в кожній із вище названих опцій, однаковий і містить у собі таке:

- формулюються цілі, які необхідно досягти в процесі виконання оціночних робіт усередині опції;
- наводиться перелік необхідних похідних даних для оцінки;
- висуваються вимоги до змісту і форми інформаційних матеріалів, які повинні бути передані Заявником у розпорядження Експерта;
- задається необхідний рівень ретельності (глибини) і деталізації наданих матеріалів, а також необхідний рівень формалізації доказів зв'язків (співвідношень) між об'єктами аналізу , що декларуються в даній опції;
- визначається зміст задач і послідовність дій Експерта в процесі виконання оціночних робіт усередині опції;
- задаються умови, що обумовлюють позитивний або негативний висновок за результатами оцінки усередині опції.

5.12 Зміст і обсяг виконуваних робіт у процесі оцінки коректності системи ТЗІ безпосередньо залежить від заявленого рівня довіри до результатів оцінки.

Чим більш високий заявлений рівень довіри, тим більш жорсткі вимоги пред'являються до формалізації і ґрунтовності оцінок коректності. Ця обставина підкреслюється у специфікаціях критеріїв дієвості шляхом вжитку дієслів "описувати"("викладати"), "пояснювати"("обґрунтовувати") і "доводити"("доказувати").

Якщо за нижчих заявлених рівнів довіри (Е1,Е2) у специфікаціях критеріїв, як правило, використовується дієслово "описувати", а за середніх рівнів (Е3,Е4)- "обґрунтовувати", то за високих рівнів довіри, в основному, необхідно "доводити" коректність тих або інших співвідношень між аналізованими об'єктами оцінки.

5.13 Стадія оцінки досягнутого рівня довіри до коректності реалізації системи ТЗІ містить у собі послідовне виконання таких чотирьох опцій:

- перевірка виконання нормативних вимог до якості документації, що описує етапи розробки, виготовлення та випробувань системи ТЗІ на оцінюваній АТС (опція 2.1);
- перевірка дотримання нормативних гарантій забезпечення захищеності інформаційних ресурсів у технологічних середовищах розробки, виготовлення та випробувань оцінюваної АТС, у т.ч. системи ТЗІ (опція 2.2);

- перевірка виконання нормативних вимог якості експлуатаційної документації на систему ТЗІ для оцінюваної АТС (опція 2.3);

- перевірка дотримання нормативних гарантій забезпечення захищеності інформаційних ресурсів експлуатаційного середовища оцінюваної АТС (опція 2.4).

5.14 Зміст робіт за опціями 2.1÷2.4 регламентований у розділі 7 цього документа.

5.15 Відповідно до цієї методики нормується сім рівнів довіри до коректності системи ТЗІ - від Е0 до Е6 Рівень довіри Е0 означає недостатню довіру до коректності. Тому є шість сукупностей довірчих критеріїв, наданих у НД ТЗІ 2.5-003-99, кожна з яких специфікує вимоги й умови одержання довірчої оцінки свого рівня.

Таким чином, усього специфікується (нормується) двадцять чотири опції оціночних робіт - чотири опції на кожному із шести рівнів довіри.

Всі довірчі критерії, що відносяться до одного оціночного рівня, містяться в окремий розділ, тобто у НД ТЗІ 2.5-003-99 є шість розділів - згідно з кількістю нормованих рівнів довіри.

5.16 Порядок викладення вимог і умов усередині будь-якої опції для кожного довірчого рівня однаковий і полягає в наступному.

Спочатку висуваються вимоги до змісту і форми інформаційних матеріалів, що повинні бути передані в розпорядження Експерта, потім вказуються ті зв'язки (співвідношення) між об'єктами оцінювання, які необхідно описувати, обґрунтовувати або доводити в поточній опції оціночних робіт, а також задається необхідний рівень глибини і деталізації описів та обґрунтувань зазначених зв'язків (співвідношень) або необхідний рівень формалізації доказів справедливості (коректності) зв'язків (співвідношень), що декларуються між об'єктами аналізу в даній опції.

Нарешті, наприкінці опції визначається зміст задач Експерта щодо перегляду коректності виконання вимог та умов.

5.17 Чим більш високий рівень довіри до коректності системи ТЗІ необхідно підтверджувати, тим більш жорсткі вимоги пред'являються щодо формалізації і ретельності обґрунтувань та доказів(див. 5.12).

5.18 Для підтвердження довірчої оцінки Заявник заздалегідь (тобто, до початку оціночних робіт) повинний надати у розпорядження Експерта всі необхідні описи, обґрунтування і докази, які відповідають заявленому рівню довіри до коректності системи ТЗІ в оцінюваній АТС. Все це потім Експерт має переглянути і видати відповідний висновок.

Експерт тільки тоді повинний надавати результати своїх власних досліджень і додаткових доказів, коли стають необхідними заходи третьої сторони (як правило, уповноваженого державного органа), щоб домогтися необхідної довіри до оцінки.

5.19 Поряд із необхідними обґрунтуваннями і доказами Заявник має надати в розпорядження Експерта тестуючі засоби, ступінь досконалості яких повинна бути адекватною заявленому рівню оцінки, а також відповідні результати тестування й інших видів випробувань.

5.20 Після виконання робіт з оцінки Експерт надає Заявнику звіт, у якому вказується результат оцінки.

5.21 У випадку негативного висновку в звіті докладно і конкретно з посиланнями на відповідні нормативні документи надаються аргументи і пояснюються причини, що спонукали Експерта зробити висновок про невідповідність результатів оцінки заявленій цілі.

5.22 У випадку позитивного висновку Експертом і Заявником спільно готуються відповідні документи, перелік яких зазначений у НД ТЗІ 2.5-003-99, для надання в уповноважений орган із метою одержання формального юридично дієвого документа, що підтверджує коректність структури системи ТЗІ на оцінюваній АТС із рівнем довіри, який відповідає зазначеному в документі нормативному рівню довіри.

5.23. Таким чином, у документі, що відбиває результати експертизи, вказується:

– структура системи ТЗІ на оцінюваній АТС у вигляді зафіксованої множини функціональних послуг захисту з реалізованими рівнями стійкості механізмів захисту, коректність якої підтверджується;

– підтверджене значення рівня довіри (у межах від Е1 до Е6) до коректності структури системи ТЗІ на АТС.

6 Оцінка коректності реалізації системи ТЗІ

6.1 Оцінка коректності структури системи ТЗІ (опція 1.1)

6.1.1 Метою оцінки коректності структури системи ТЗІ є встановлення факту, чи дійсно структура системи захисту, що надана у вигляді взаємопов'язаної множини ФПЗ із зазначеними рівнями стійкості механізмів реалізації цих послуг, може забезпечити очікуваний рівень захищеності інформаційних ресурсів на АТС.

6.1.2 Необхідними даними для оцінки є:

- заявлений рівень захищеності інформаційних ресурсів АТС, сформульований у термінах моделі загроз, тобто у вигляді переліка суттєвих загроз для інформації із зазначеними гранично припустимими рівнями втрат від їхніх можливих реалізацій;
- перелік ФПЗ, що включені у модель захисту;
- перелік механізмів захисту з зазначеними рівнями їхньої стійкості;
- аналіз придатності ФПЗ, що включені у модель захисту, протистояти суттєвим загрозам;
- аналіз взаємодій ФПЗ між собою;
- аналіз відомих "слабких місць" у структурі системи захисту.

6.1.3 У випадках високих заявлених рівнів довірчої оцінки (починаючи з рівня Е4 і вище) Заявник зобов'язаний надати Експертові опис технічної політики безпеки і передати в розпорядження Експерта додаткову інформацію, пов'язану з аналізом середовища функціонування АТС (див. НД ТЗІ 2.7-001-99), побудовою моделей порушників, побудовою й аналізом моделі загроз, аналізом ризиків, обґрунтуванням необхідного рівня

захищеності інформаційних ресурсів на АТС у конкретних або передбачуваних умовах експлуатації. Ступінь повноти і ретельності наданих у цих випадках матеріалів залежить від очікуваного рівня довіри до коректності системи ТЗІ на оцінюваній АТС. На рівні Е4 технічну політику безпеки дозволяється надавати в описовій формі. На рівні Е5 опис технічної політики безпеки повинен містити напівформальне уявлення її основних елементів. На рівні Е6 повинен бути наданий формальний опис прийнятої політики безпеки на оцінюваній АТС.

6.1.4 Вище названі дані Заявник надає у розпорядження Експерта.

Зміст і форма наданих матеріалів залежить від очікуваного рівня довірчої оцінки і визначається у специфікаціях згідно НД ТЗІ 2.5-003-99. Щонайменше, повинна бути надана вся інформація, що зазначена в таблиці 1 для заявленого рівня довірчої оцінки.

6.1.5 Аналіз придатності ФПЗ має показати, яким чином послуги захисту протидіють суттєвим загрозам.

У аналізі повинна бути обґрунтована функціональна повнота моделі захисту, тобто повинно бути показано, що не є хоча б одна суттєва загроза, для якої не була б організована протидія за допомогою хоча б однієї ФПЗ. Також повинний бути виконаний аналіз домірності гранично припустимих втрат від можливих проявів загроз і запропонованих до реалізації рівнів стійкості механізмів захисту, що протидіють цим загрозам.

Таблиця 1

Відомості, що використовуються в процесі оцінки коректності системи ТЗІ						
Об'єкт, що потребує аналізу в процесі оцінки	Заявлені рівні довірчих оцінок коректності системи ТЗІ на АТС					
	Е1	Е2	Е3	Е4	Е5	Е6
Технічне завдання на систему ТЗІ	-	*	*	*	*	*
Технічна політика безпеки	-	-	-	*	*	*
Неформальні специфікації функціональних послуг захисту	*	*	*	*	*	*
Напівформальні специфікації функціональних послуг захисту	-	-	-	*	*	-
Формальні специфікації функціональних послуг захисту	-	-	-	-	-	*
Неформальні специфікації технічного проекту	*	*	*	-	-	-
Напівформальні специфікації технічного проекту	-	-	-	*	*	-
Формальні специфікації технічного проекту	-	-	-	-	-	*
Неформальні специфікації робочого проекту	-	*	-	-	-	-
Напівформальні специфікації робочого проекту	-	-	-	*	*	*
Комплект конструкторської документації на технічні засоби АТС	-	-	-	*	*	*
Лістинги (коди програм ЕОМ) об'єктів програмного забезпечення	-	-	-	*	*	*

Закінчення таблиці 1

Відомості, що використовуються в процесі оцінки коректності системи ТЗІ						
Об'єкт, що потребує аналізу в процесі оцінки	Заявлені рівні довірчих оцінок коректності системи ТЗІ на АТС					
	Е1	Е2	Е3	Е4	Е5	Е6
Ключова інформація об'єктів і суб'єктів	-	-	-	-	-	*
Умови експлуатації (експлуатаційна документація, умови поставки, конфігурування, інсталювання, введення в експлуатацію і т.ін.)	*	*	*	*	*	*
Рівень вимог до глибини та деталізації наданих Заявником матеріалів	Рівень опису і, можливо, короткого пояснення		Рівень детального пояснення та обґрунтування		Рівень доказів	

Примітка: символ "*" ("зірочка"), занесений у певний квадрат таблиці 1, означає, що на об'єкт аналізу, який відповідає рядку, де зазначена "зірочка", поширюються умови, які специфіковані найменуванням обраного "зірочкою" стовпця.

6.1.6 Аналіз взаємодій ФПЗ між собою має показати всі можливі відношення між ними, обґрунтувати раціональність взаємозв'язків послуг захисту в моделі з точки зору виключення зайвого дублювання або надлишкового використання ресурсів, мінімізації витрат на захист і т.ін.

Також має бути показано, що послуги захисту не вступають у конфлікт або у внутрішню протидію між собою.

Нарешті, повинно бути показано, що ФПЗ, які включені в модель захисту, взаємно підтримують один одного, утворюють єдине діюче ціле.

6.1.7 Аналіз відомих "слабких місць" у структурі системи захисту має показати:

- усі можливі шляхи і негативні наслідки їхніх проявів;
- заходи щодо нейтралізації або зменшення наслідків таких проявів.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) повинні бути надані пояснення або доказ, чому аналізоване "слабке місце" не впливає на політику безпеки на АТС .

6.1.8 Задача Експерта в процесі оцінки коректності структури системи захисту полягає у перегляді того, чи усі вимоги щодо повноти і коректності змісту та форми наданих матеріалів, а також поданих обгрунтувань і доказів виконані у аналізах придатності, взаємодій і "слабких місць".

Експерт має переглянути, чи всі надані відомості відповідають зазначеним у таблиці 1 для потрібного рівня оцінки.

6.1.9 Послідовність дій Експерта в процесі оцінки коректності структури системи захисту показана на рисунку 2 і містить у собі:

- перегляд результатів аналізу функціональної достатності моделі захисту;
- перегляд результатів аналізу якості взаємодій ФПЗ між собою, тобто результатів оцінки функціональної надмірності моделі захисту;
- перегляд результатів аналізу відомих "слабких місць" у структурі системи захисту.

6.1.10 У процесі перегляду результатів аналізу функціональної достатності моделі захисту Експерт повинен переконатися, що:

- відсутня хоча б одна загроза, із множини включених у перелік суттєвих загроз, для якої не була б організована протидія за допомогою хоча б однієї ФПЗ, із множини включених у модель захисту;

- рівні стійкості запропонованих до реалізації механізмів захисту достатні, щоб втрати від можливих реалізацій загроз не перевищили гранично припустимих рівнів втрат.

6.1.11 У процесі перегляду результатів аналізу якості взаємодій ФПЗ між собою Експерт повинен переконатися, що:

- рівні стійкості запропонованих до реалізації механізмів захисту домірні до гранично припустимих втрат від можливих реалізацій загроз, котрим ці механізми протидіють;

- виключене зайве дублювання ФПЗ;

- у моделі захисту відсутні зайві ФПЗ;

- включені у модель захисту ФПЗ не вступають у конфлікт між собою;

- включені у модель захисту ФПЗ взаємно підтримують один одного і утворюють єдине діюче ціле.

6.1.12 У процесі перегляду результатів аналізу відомих "слабких місць" у структурі системи захисту Експерт повинен переконатися, що:

- усі потенційно можливі "слабкі місця" у структурі моделі захисту виявлені і враховані у відомості (переліку) "слабких місць";

- рівні негативних наслідків від можливих проявів виявлених "слабких місць" не перевищують оцінок Заявника.

У процесі перегляду Експерт може зробити власний аналіз "слабких місць". Перевірити ще раз, чи усі комбінації "слабких місць" були досліджені.

Кожне "слабке місце" у структурі системи захисту повинно бути переглянуто з позицій повноти обліку каналів стикання "слабкого місця" із зовнішнім середовищем.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) Експерт повинний виконати тестування відомих "слабких місць" у структурі системи захисту.

6.1.13 Структура системи захисту вважається коректною, якщо у наданих матеріалах не будуть знайдені помилки, неточності, нерозтлумачені положення і спірні твердження, а самі матеріали будуть задовольняти Експерта відносно ступеня повноти і глибини змісту.

6.1.14 Структура системи захисту вважається некоректною, якщо в розпорядження Експерта на період оціночних робіт була надана не вся необхідна інформація, або якщо в наданих матеріалах була знайдена хоча б одна помилка, неточність, нерозтлумачене положення або спірне твердження, які Заявник в обговорені терміни до кінця оціночних робіт не зумів усунути.

6.1.15 Якщо Заявник вважає за можливе передати у розпорядження Експерта технічне завдання і технічний проект системи ТЗІ для оцінюваної АТС, то не потрібно оформляти дані для оцінки коректності структури системи захисту у вигляді аналізу придатності й аналізу взаємодій, оскільки всі необхідні відомості для виконання оціночних робіт містяться в технічному завданні й у технічному проекті системи ТЗІ.

Рисунок 2 – Опція 1.1. Оцінка коректності структури системи ТЗІ на АТС.

Послідовність дій Експерта

6.2 Оцінка коректності проекту КЗМЗ

6.2.1 Метою оцінки коректності проекту комплексу засобів і механізмів захисту (КЗМЗ) є встановлення факту, чи дійсно проект КЗМЗ коректно реалізує задану модель захисту інформації на АТС від загроз, що створюються через технічні канали.

6.2.2 Необхідними даними для оцінки є:

- перелік ФПЗ, що включені в модель захисту;
- перелік механізмів захисту з зазначеними рівнями стійкості їхніх реалізацій;
- специфікації ФПЗ, що нормовані для програмно-керованих АТС загального користування (див. НД ТЗІ 2.5-003-99);
- аналіз функціональної достатності проекту КЗМЗ;
- аналіз взаємодій засобів і механізмів захисту (із метою усунення надмірності) у проекті КЗМЗ;
- аналіз відомих "слабких місць" у проекті КЗМЗ.

6.2.3 У випадках високих заявлених рівнів довірчої оцінки (починаючи з рівня Е4 і вище) Заявник зобов'язаний надати Експерту матеріали робочого проектування як системи ТЗІ, так і програмно-технічних засобів АТС у цілому - конструкторських креслень і принципових схем технічних засобів, лістингів програм, спеціалізованих тестів і т. ін.

6.2.4 Вище називані дані, окрім нормативно затверджених специфікацій, Заявник надає у розпорядження Експерта.

Зміст і форма наданих матеріалів залежить від очікуваного рівня довірчої оцінки щодо коректності. Щонайменше, має бути надана вся інформація, що зазначена в таблиці 1 для потрібного заявочного рівня.

6.2.5 Аналіз функціональної достатності проекту КЗМЗ повинний показати, яким чином ФПЗ реалізовані в проекті КЗМЗ.

У аналізі має бути обґрунтована функціональна повнота проекту КЗМЗ, тобто повинно бути показано, що усі ФПЗ, які включені в модель захисту, реалізовані в проекті КЗМЗ. При цьому зміст реалізованих послуг захисту повинен відповідати нормованим специфікаціям (див. НД ТЗІ 2.5-003-99) із метою виключення неоднозначності в розумінні змісту функціонування таких послуг.

6.2.6 Аналіз взаємодій засобів і механізмів захисту в проекті КЗМЗ повинен показати всі можливі співвідношення між ними, обґрунтувати раціональність взаємозв'язки засобів і механізмів захисту в проекті, маючи на увазі виключення зайвого дублювання, надлишкового використання ресурсів, мінімізацію витрат на захист і т. ін.

Тут же повинно бути показано, що реалізовані механізми захисту не вступають у конфлікт між собою, взаємно підтримують один одного й утворюють єдине діюче ціле.

6.2.7 Аналіз відомих "слабких місць" у проекті КЗМЗ має показати всі можливі шляхи і негативні наслідки їхніх проявів, заходи щодо нейтралізації або зменшення наслідків таких проявів.

У необхідних випадках повинні бути надані пояснення або доказ, чому аналізоване "слабке місце" не впливає на політику безпеки на АТС .

6.2.8 Задача Експерта в процесі оцінки коректності проекту КЗМЗ полягає в перегляді того, чи усі вимоги щодо повноти і коректності змісту і форми описів, обґрунтувань і доказів виконані в процесі аналізу функціональної достатності, взаємодій засобів і механізмів захисту і "слабких місць" у проекті КЗМЗ.

Експерт має переглянути також, чи вся інформація застосована, що зазначена в табл.1 для потрібного рівня оцінки.

6.2.9 Послідовність дій Експерта в процесі оцінки коректності проекту КЗМЗ показана на рисунку 3 і містить у собі:

- перегляд результатів аналізу функціональної достатності проекту КЗМЗ;
- перегляд результатів аналізу якості взаємодій засобів і механізмів захисту між собою, тобто результатів аналізу функціональної надмірності проекту КЗМЗ;
- перегляд результатів аналізу відомих "слабких місць" у проекті КЗМЗ.

6.2.10 У процесі перегляду результатів аналізу функціональної достатності проекту КЗМЗ Експерт має переконатися, що:

- відсутня хоча б одна ФПЗ, що включена в модель захисту і не була б реалізована в проекті за допомогою певних засобів або механізмів захисту;
- рівні стійкості запроектованих механізмів захисту відповідають запропонованим до реалізації в моделі захисту;
- зміст запроектованих функцій і механізмів захисту відповідає нормативно затвердженим специфікаціям НД ТЗІ 2.5-001-99.

6.2.11 У процесі перегляду результатів аналізу якості взаємодій засобів і механізмів захисту в проекті КЗМЗ Експерт повинен переконатися, що:

- рівні стійкості запроектованих механізмів захисту є мінімально необхідними для реалізації прийнятої моделі захисту;
- виключене зайве дублювання засобів і механізмів захисту;
- включені до проекту засоби і механізми захисту не вступають у конфлікт між собою;
- включені до проекту засоби і механізми захисту взаємно підтримують один одного й утворюють єдине діюче ціле.

6.2.12 У процесі перегляду результатів аналізу відомих "слабких місць" у проекті КЗМЗ Експерт повинен переконатися, що:

- усі потенційно можливі "слабкі місця" у проекті КЗМЗ виявлені і враховані у відомості (переліку) "слабких місць";
- рівні негативних наслідків від можливих проявів виявлених "слабких місць" не перевищують оцінок Заявника.

У процесі перегляду Експерт може зробити власний аналіз "слабких місць". Перевірити ще раз, чи усі комбінації "слабких місць" були досліджені.

Кожне "слабке місце" у проекті КЗМЗ повинно бути перепровірене з позицій повноти обліку каналів стикання "слабкого місця" із зовнішнім середовищем.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) Експерт повинен виконати тестування відомих "слабких місць" у проекті КЗМЗ.

6.2.13 Проект КЗМЗ вважається коректним, якщо в наданих матеріалах не будуть знайдені помилки, неточності, нерозтлумачені положення і спірні твердження, а самі матеріали будуть задовольняти Експерта ступенем повноти і глибини змісту.

6.2.14 Проект КЗМЗ вважається некоректним, якщо в розпорядження Експерта на період оціночних робіт була надана не вся необхідна інформація, або якщо в наданих матеріалах була знайдена хоча б одна помилка, неточність, не розтлумачене положення або спірне твердження, які Заявник в обговорені терміни до кінця оціночних робіт не зумів усунути.

6.2.15 Якщо Заявник вважає за можливе передати в розпорядження Організатора експертизи технічну документацію щодо побудови моделей порушників, розробки технічного завдання і техно-робочого проекту системи ТЗІ на АТС , то не потрібно оформляти дані для оцінки коректності проекту КЗМЗ у вигляді переліків послуг і механізмів захисту, обґрунтувань або доказів повноти реалізацій послуг захисту й інших вище названих аналізів, оскільки всі необхідні відомості для виконання оцінки містяться в технічному

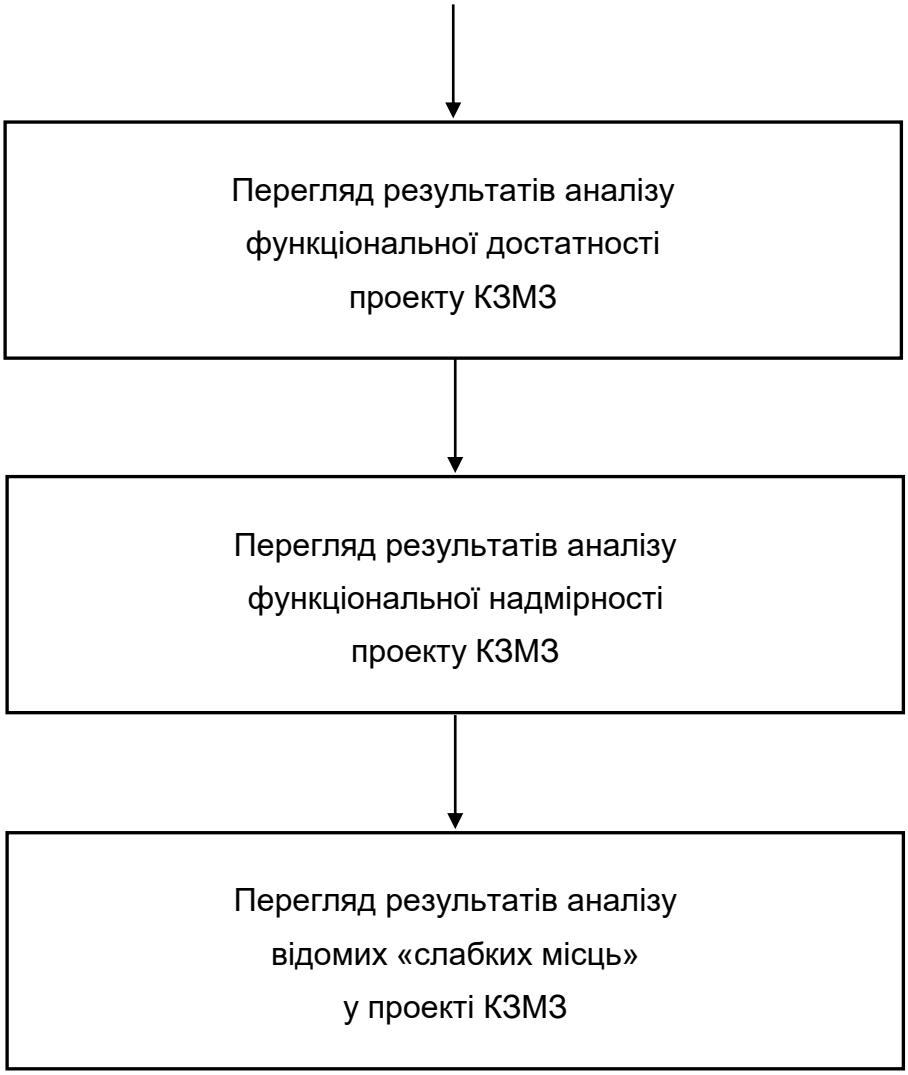

Рисунок 3 – Опція 1.2. Оцінка коректності проекту щодо створення КЗМЗ на АТС..

Послідовність дій Експерта

6.3 Оцінка коректності реалізації КЗМЗ

6.3.1 Метою оцінки коректності реалізації КЗМЗ є установлення факту, чи дійсно наявний у складі оцінюваної АТС КЗМЗ у визначених умовах експлуатації реально функціонує відповідно до проектної документації та нормованих специфікацій функціональних послуг і механізмів захисту (див. НД ТЗІ 2.5-001-99).

6.3.2 Вихідними необхідними даними для оцінки є:

- перелік ФПЗ, які включені Заявником у модель захисту;
- перелік наданих у проекті механізмів захисту з зазначеними рівнями стійкості їхніх реалізацій;
- нормовані специфікації ФПЗ для АТС (див. НД ТЗІ 2.5-001-99);
- програма та методика випробувань оцінюваного КЗМЗ;
- аналіз та протоколи випробувань стійкості реалізованих механізмів захисту;
- аналіз та протоколи випробувань відомих" слабких місць" у конструкції АТС, включаючи систему ТЗІ;

- аналіз та протоколи випробувань відомих " слабких місць" в експлуатації оцінюваної АТС;

- програма та методика вимірювань параметрів технологічного середовища експлуатації оцінюваної АТС після проведення заходів захисту (тобто, програма та методика проведення так званих "спецдосліджень" середовища експлуатації);

Зміст випробувань та вимірювань повинен відповідати ГОСТ 2.106.96.

Протоколи випробувань та вимірювань мають бути надані в обсязі, що залежить від очікуваного рівня довіри і відповідає вимогам цього НД та НД ТЗІ 2.5-003-99.

6.3.3 У випадках високих заявлених рівнів довірчої оцінки (починаючи з рівня Е4 і вище) Заявник зобов'язаний надати Організатору експертизи матеріали приймально-здавальних випробувань, матеріали робочого проектування як системи ТЗІ, так і програмно-технічних засобів АТС у цілому - конструкторських креслень і принципових схем технічних засобів, лістингів програм, спеціалізованих тестів і т. ін.

Заявник також зобов'язаний на вимогу Організатора експертизи забезпечити проведення додаткових випробувань із метою уточнення деталей функціонування того або іншого механізму захисту.

6.3.4 Вище називані дані, крім нормативно затверджених специфікацій, Заявник надає в розпорядження Організатора експертизи.

Зміст і форма наданих матеріалів залежить від потрібного рівня довірчої оцінки коректності.

Щонайменше, має бути надана вся інформація, що зазначена в таблиці 1 для потрібного заявочного рівня.

6.3.5 Аналіз стійкості реалізованих механізмів захисту повинний показати, що вони в реальних умовах функціонування АТС на практиці забезпечують проектні рівні стійкості при безпосередньому (прямому) впливі загроз.

У аналізі повинна бути обґрунтована функціональна повнота реалізованого КЗМЗ, тобто має бути показано, що проект КЗМЗ у повному обсязі реалізований на практиці. При цьому зміст реалізованих механізмів захисту повинний точно відповідати нормуючим специфікаціям (див. НД ТЗІ 2.5-001-99).

6.3.6 Аналіз реальних характеристик технологічного середовища експлуатації захищеної АТС повинний показати, що після проведення заходів захисту параметри реальних характеристик експлуатаційного середовища знаходяться у припустимих діапазонах значень.

Повинні бути надані результати вимірів інформативних параметрів побічних електромагнітних випромінювань і навідів (ПЕМВН) від елементів абонентських ліній зв'язку, каналів зв'язку станційного устаткування з виносами, терміналів, принтерів і інших технічних засобів АТС до і після проведення заходів захисту.

Повинні бути надані результати вимірів інформативних параметрів електромагнітних навідів в елементах АТС від розташованих у зонах, що захищаються, сторонніх джерел інформативних випромінювань.

Повинні бути надані результати вимірів інформативних параметрів сигналів побічних акусто-електричних перетворень в абонентських і системних прикінцевих пристроях.

У випадках проведення спеціальних досліджень на технічних каналах витоку інформації, для яких є затверджені (атестовані) програми та (або) методики вимірів і випробувань, необхідно користуватися тільки затвердженими програмами та (або) методиками.

У випадках проведення спеціальних досліджень на технічних каналах, для яких відсутня відповідна нормативна база вимірів і випробувань, необхідно методи і схеми вимірів, що мають бути використані, погоджувати з уповноваженим державним органом.

Значення обмірюваних характеристик експлуатаційного середовища АТС не повинні перевищувати нормованих значень на межах контрольованих зон.

6.3.7 Аналіз відомих " слабких місць" у конструкції АТС повинний показати:

- усі можливі шляхи і негативні наслідки їхніх проявів;
- заходи щодо нейтралізації або зменшення наслідків таких проявів.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) повинні бути надані пояснення або докази, чому аналізоване " слабке місце" не впливає на політику безпеки на АТС .

6.3.8 Аналіз відомих " слабких місць" у процесі експлуатації оцінюваної АТС повинний показати:

- усі можливі шляхи і негативні наслідки їхніх проявів;
- заходи щодо нейтралізації або зменшення наслідків таких проявів.

Аналіз " слабких місць" у процесі експлуатації повинен показати також, що будь-які помилкові і (або) зловмисні дії користувачів і персоналу в процесі взаємодії з АТС однозначно розпізнаються системою, що відсутня можливість реконфігурації АТС із боку не уповноважених осіб, при котрій хоч який-небудь засіб або механізм захисту переводиться у пасивний непрацездатний стан або сфера дії його обмежується.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) повинні бути надані пояснення або докази, чому аналізоване " слабке місце"не впливає на політику безпеки АТС, або чому воно не може проявитися в даних конкретних умовах експлуатації.

У випадку використання криптографічних механізмів їхня стійкість повинна бути оцінена службою, що має повноваження на виконання таких робіт.

6.3.9 Задача Експерта в процесі оцінки коректності реалізації КЗМЗ полягає в перегляді того, чи усі вимоги щодо повноти і коректності змісту і форми описів, обґрунтувань і доказів виконані при визначенні коректності реалізації системи захисту на оцінюваній АТС.

Необхідно перевірити також, чи всі надані відомості відповідають зазначеним у таблиці 1 для потрібного рівня оцінки.

6.3.10 Послідовність дій Експерта в процесі оцінки коректності реалізації КЗМЗ показана на рисунку 4 і містить у собі:

- перегляд результатів аналізу стійкості реалізованих механізмів захисту;
- перегляд результатів аналізу реальних характеристик технологічного середовища експлуатації АТС після проведення заходів захисту;
- переперевірку результатів аналізу відомих "слабких місць" у конструкції АТС, включаючи систему ТЗІ;
- перегляд результатів аналізу відомих "слабких місць" в експлуатації АТС.

Рисунок 4 – Опція 1.3. Оцінка коректності реалізації КЗМЗ.

Послідовність дій Експерта

6.3.11 У процесі перегляду результатів аналізу стійкості Експерт повинний переконатися, що:

- усі запроектовані механізми захисту в повному обсязі реалізовані на практиці;
- рівні стійкості реалізованих механізмів захисту відповідають проектній документації;
- зміст реалізованих механізмів захисту відповідає нормативно затвердженим специфікаціям (див. НД ТЗІ 2.5-001-99).

6.3.12. У процесі перегляду результатів аналізу реальних характеристик експлуатаційного середовища АТС після проведення заходів захисту Експерт повинний переконатися, що:

- у наданому аналізі враховані всі характеристики середовища експлуатації, що мають відношення до проявів суттєвих загроз для інформації з боку технічних каналів;
- параметри реальних характеристик експлуатаційного середовища (ПЕМВН, сигнали побічних акусто-електричних перетворень і т.ін.) знаходяться в припустимих діапазонах значень;
- аналіз і виміри параметрів середовища виконувалися згідно затверджених і (або) погоджених із боку уповноважених органів методик.

6.3.13 У процесі перегляду результатів аналізу відомих " слабких місць" у конструкції АТС Експерт повинний переконатися, що:

- усі потенційно можливі " слабкі місця" у конструкції АТС, включаючи систему ТЗІ, виявлені і враховані у відомості (переліку) "слабких місць" ;
- рівні негативних наслідків від можливих проявів виявлених " слабких місць" не перевищують оцінок Заявника.

У процесі перегляду Експерт може зробити власний аналіз "слабких місць" у конструкції АТС. Перевірити, чи усі комбінації "слабких місць" були досліджені.

Кожне "слабке місце" у проекті КЗМЗ повинно бути перевірене з урахуванням повноти обліку каналів стикання "слабкого місця" із зовнішнім середовищем.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) Експерт повинний виконати тестування відомих "слабких місць" у конструкції АТС, включаючи систему ТЗІ.

6.3.14 У процесі перегляду результатів аналізу відомих "слабких місць" щодо експлуатації АТС Експерт повинний переконатися, що:

- усі потенційно можливі " слабкі місця" у процесі експлуатації виявлені і враховані у відомості (переліку) "слабких місць";
- рівні негативних наслідків від можливих проявів виявлених "слабких місць" не перевищують оцінок Заявника.

У процесі перегляду Експерт може зробити власний аналіз "слабких місць", що виникають на етапі експлуатації АТС. Переглянути, чи усі комбінації "слабких місць" були досліджені.

Кожне "слабке місце" у проекті КЗМЗ повинно бути перевірене з урахуванням повноти обліку каналів стикання "слабкого місця" із зовнішнім середовищем.

У необхідних випадках (див. НД ТЗІ 2.5-003-99) Експерт повинний виконати тестування відомих "слабких місць" у процесі експлуатації АТС.

6.3.15 Реалізація КЗМЗ вважається коректною, якщо результати аналізів стійкості реалізованих механізмів захисту, реальних характеристик технологічного середовища АТС і відомих "слабких місць" виявляться позитивними, у наданих матеріалах не будуть знайдені помилки, неточності, не розтлумачені положення і спірні твердження, а самі матеріали будуть задовольняти Експерта за ступенем повноти і глибини змісту.

6.3.16 Реалізація КЗМЗ вважається некоректною, якщо в розпорядження Експерта на період оціночних робіт була подана не вся необхідна інформація, або якщо в наданих матеріалах була знайдена хоча б одна помилка, неточність, не розтлумачене положення або спірне твердження, які Заявник в обговорені терміни до кінця оціночних робіт не зумів усунути.

7 Оцінка рівня довіри до коректності реалізації системи ТЗІ

7.1 Висновок про коректність реалізованої системи ТЗІ на оцінюваній АТС може бути зроблений, як це випливає, наприклад, з аналізу таблиці 1, на базі різної повноти і глибини знань про неї. Тому і рівень довіри до результатів оцінки коректності може бути різним.

7.2 Метою оцінки рівня довіри до коректності реалізації системи ТЗІ є підтвердження або спростування вказаного Заявником у заявочних документах ступеня впевненості у тому, що реалізована на оцінюваній АТС система ТЗІ забезпечує необхідний Заявникові рівень захищеності інформаційних ресурсів.

7.3 Якщо оцінка коректності реалізації системи ТЗІ, що виконана відповідно до положень розділу 6, дала позитивний результат, то мета оцінки рівня довіри зводиться до підтвердження або спростування заявленого ступеня впевненості до отриманого висновку про коректність реалізації системи ТЗІ на оцінюваній АТС.

7.4 У цьому документі специфікується сім можливих рівнів довіри (сім градацій в оцінці ступеня довіри) до коректності системи ТЗІ, як-от рівні довіри Е0, Е1, Е2, Е3, Е4, Е5 і Е6.

7.5 Найнижчий рівень довірчої оцінки - Е0 означає недостатню довіру до коректності реалізації системи ТЗІ на оцінюваній АТС.

7.6 Рівень довіри Е1 є початковим рівнем, нижче якого раціональна довіра не зберігається. Для підтвердження довірчої оцінки Е1 Заявнику досить надати матеріали технічного завдання на розробку системи ТЗІ і неформального опису технічного проекту.

7.7 На оціночному рівні Е2 необхідно, на додаток до вищевказаних матеріалів, представити неформальний опис матеріалів робочого проекту. Має бути оцінена змістовність функціональних тестів. Повинен бути наданий опис системи керування доступом, розподілу ресурсів і повноважень, а також засобів конфігурування АТС.

7.8 Додатково до вимог для рівня Е2 на оціночному рівні Е3 повинен бути наданий не тільки опис, але і детальне пояснення й обґрунтування використовуваних на АТС програмних і технічних засобів і механізмів захисту. Повинна бути надана оцінка повноти і змістовності тестів системи ТЗІ.

7.9 На оціночному рівні Е4, на додаток до вище зазначених матеріалів, повинно бути надане в описовій формі обґрунтування прийнятої технічної політики безпеки. Повинні бути надані докладні матеріали техно-робочого проекту, включаючи лістинги програм і конструкторську документацію, із докладним обґрунтуванням основних прийнятих рішень.

7.10 На оціночному рівні Е5 має бути надана практично вся інформація, що пов'язана з розробкою, виготовленням і експлуатацією АТС. Повинна бути доведена, при можливості у формалізованому вигляді, коректність усіх прийнятих наукових, технічних і конструкторських рішень на всіх стадіях життєвого циклу станції.

7.11 На вищому оціночному рівні Е6, на додаток до вимог для рівня Е5, повинен бути наданий формальний опис прийнятої моделі політики безпеки на АТС .

7.12 Основним змістом робіт з оцінки рівня довіри до коректності реалізації системи ТЗІ є:

- послідовний перегляд конструкторської й експлуатаційної документації на відповідність нормуючим специфікаціям, які викладені у НД ТЗІ 2.5-003-99 для очікуваного рівня довіри;
- послідовний перегляд на очікуваному рівні довіри дотримання нормованих у НД ТЗІ 2.5-003-99 гарантій забезпечення захищеності інформації в технологічних середовищах створення й існування АТС на всіх стадіях її життєвого циклу.

7.13 Довірчі критерії підрозділяються на чотири групи:

- вимоги до документації, що містить результати розробки, виготовлення та випробувань системи ТЗІ на оцінюваній АТС (опція 2.1);
- гарантії забезпечення інформаційної захищеності середовищ розробки, виготовлення та випробувань оцінюваної АТС, у тому числі і системи ТЗІ на ній (опція 2.2);
- вимоги до експлуатаційної документації на систему ТЗІ для оцінюваної АТС (опція 2.3);
- гарантії забезпечення інформаційної захищеності експлуатаційного середовища на оцінюваній АТС (опція 2.4).

7.14 У першій групі довірчих критеріїв (опція 2.1) специфікуються вимоги до документації, що містить результати розробки, виготовлення та випробувань системи ТЗІ на оцінюваній АТС, тобто визначаються вимоги до документації на створення системи ТЗІ, які необхідно виконати, щоб мати можливість формального віднесення оцінюваної системи до одного із шістьох нормованих рівнів довіри.

7.15 Необхідними даними для оцінки якості документованості процесу створення системи ТЗІ є:

- матеріали технічного завдання на систему ТЗІ;
- матеріали технічного проектування системи ТЗІ;
- матеріали робочого проектування системи ТЗІ;
- документація щодо виготовлення та випробувань системи ТЗІ.

7.16 Вище називані дані Заявник надає у розпорядження Організатора експертизи.

Зміст і форма наданих матеріалів залежить від очікуваного рівня довірчої оцінки коректності і визначається у специфікаціях НД ТЗІ 2.5-003-99.

7.17 У процесі оцінки якості документованості за опцією 2.1 аналізуються чотири аспекти:

- якість документованості стадії розробки технічного завдання на систему ТЗІ для оцінюваної АТС (аспект 2.1.1);
- якість документованості стадії технічного проекту на систему ТЗІ для оцінюваної АТС (аспект 2.1.2);
- якість документованості стадії робочого проекту на систему ТЗІ для оцінюваної АТС (аспект 2.1.3);
- якість документованості стадій виготовлення та випробувань системи ТЗІ для оцінюваної АТС (аспект 2.1.4).

7.18 Задачі Експерта в процесі оцінки якості документованості за опцією 2.1 полягають у послідовному перегляді дотримання вимог і умов, що специфіковані у НД ТЗІ 2.5-003-99.

7.19 Якість документованості процесу створення АТС і системи ТЗІ для неї вважається достатньою, якщо надані матеріали відповідають специфікаціям довірчих оцінок для потрібного рівня довіри (див. НД ТЗІ 2.5-003-99).

7.20 Якість документованості процесу створення АТС і системи ТЗІ для неї вважається недостатньою, якщо у розпорядження Експерта на період оціночних робіт була надана не вся необхідна інформація, або якщо в наданих матеріалах є невідповідність нормуючим специфікаціям, яку Заявник в обговорені терміни не зумів усунути.

7.21 Друга група довірчих критеріїв пов'язана з одержанням гарантій того, що захищеність інформації в середовищах розробки, виготовлення та випробувань оцінюваної АТС належним чином забезпечена.

У НД ТЗІ 2.5-003-99 наводяться специфікації рівнів довіри до середовищ розробки, виготовлення та випробувань АТС, тобто визначаються вимоги до середовища створення АТС, які необхідно виконати, щоб мати можливість формального віднесення оцінюваної системи до одного із шести нормованих рівнів довіри.

7.22 Вихідними необхідними даними для оцінки захищеності інформації в середовищі створення АТС і системи ТЗІ для неї є:

- матеріали з описом реалізованих гарантій безпеки середовища творців оцінюваної АТС і системи ТЗІ для неї;
- матеріали з описом реалізованих гарантій фізичної захищеності середовища створення оцінюваної АТС і системи ТЗІ для неї;

- матеріали з описом реалізованих гарантій стандартизованості середовища створення оцінюваної АТС і системи ТЗІ для неї;

- матеріали з описом реалізованих гарантій спостережності і керованості середовища створення оцінюваної АТС і системи ТЗІ для неї;

- матеріали з описом реалізованих гарантій забезпечення конфіденційності і цілісності інформаційних ресурсів у середовищі створення оцінюваної АТС і системи ТЗІ для неї;

- матеріали з описом реалізованих гарантій якості документації на середовище створення оцінюваної АТС.

7.23 Вище називані дані Заявник надає у розпорядження Організатора експертизи.

Зміст і форма наданих матеріалів залежить від очікуваного рівня довірчої оцінки коректності і визначається у специфікаціях, що наведені у НД ТЗІ 2.5-002-99 і НД ТЗІ 2.5-003-99.

7.24 У процесі оцінки захищеності інформації в середовищі створення АТС аналізується шість аспектів:

- гарантії безпеки середовища творців АТС і системи ТЗІ для неї (аспект 2.2.1);

- гарантії фізичної захищеності середовища створення АТС і системи ТЗІ для неї (аспект 2.2.2);

- гарантії стандартизованості середовища створення АТС і системи ТЗІ для неї (аспект 2.2.3);

- гарантії спостережності і керованості середовища створення АТС і системи ТЗІ для неї (аспект 2.2.4);

- гарантії забезпечення конфіденційності і цілісності інформаційних ресурсів у середовищі створення АТС і системи ТЗІ для неї (аспект 2.2.5);

- гарантії якості документації на середовище створення АТС і системи ТЗІ для неї (аспект 2.2.6).

Оскільки система ТЗІ може створюватися автономно від інших елементів АТС, а вимоги до захищеності середовища створення системи ТЗІ можуть істотно відрізнятися від подібних вимог до середовища створення самої АТС, то в НД ТЗІ 2.5-003-99 вище називані середовища специфікуються роздільно.

7.25 Задача Експерта в процесі оцінки захищеності середовища створення АТС, зокрема, і середовища створення системи ТЗІ для неї, полягає у послідовному перегляді дотримання вимог і умов, що специфіковані у НД ТЗІ 2.5-002-99 і НД ТЗІ 2.5-003-99.

7.26 Якість захищеності середовища створення АТС і системи ТЗІ для неї вважається достатньою, якщо надані матеріали відповідають специфікаціям гарантій захисту і довірчих оцінок щодо заявленого рівня довіри (див. НД ТЗІ 2.5-002-99 і НД ТЗІ 2.5-003-99).

7.27 Якість захищеності середовища створення АТС і системи ТЗІ для неї вважається недостатньою, якщо у розпорядження Експерта на період оціночних робіт була надана не вся необхідна інформація, або якщо в наданих матеріалах є невідповідність нормованим специфікаціям, або якщо Заявник в обговорені терміни до кінця оціночних робіт не зумів ці невідповідності усунути.

7.28 У третій групі довірчих критеріїв (опція 2.3) специфікуються вимоги до документації, що містить опис шляхів безпечної експлуатації оцінюваної АТС, тобто визначаються вимоги до експлуатаційної документації, які необхідно виконати, щоб мати можливість формального віднесення оцінюваної системи до одного із шести нормованих рівнів довіри.

7.29 Необхідними даними для оцінки якості експлуатаційної документації є:

- документація користувача оцінюваної АТС;
- документація адміністратора оцінюваної АТС.

7.30 Вище називані дані Заявник надає у розпорядження Організатора експертизи.

Зміст і форма наданих документів залежить від очікуваного рівня довірчої оцінки коректності і визначається в специфікаціях, що наведені у НД ТЗІ 2.5-003-99.

7.31 У процесі оцінки якості документованості експлуатаційного середовища за опцією 2.3 аналізуються два аспекти:

- якість експлуатаційної документації для обслуговуючого персоналу станції (аспект 2.3.1);
- якість експлуатаційної документації для системного адміністратора, у т.ч., можливо, для адміністратора безпеки АТС (аспект 2.3.2).

7.32 Задача Експерта в процесі оцінки якості документованості експлуатаційного середовища в рамках опції 2.3 полягає у послідовному перегляді дотримання вимог і умов, що специфіковані у НД ТЗІ 2.5-003-99.

7.33 Якість документованості експлуатаційного середовища оцінюваної АТС вважається достатньою, якщо надані матеріали відповідають специфікаціям довірчих оцінок щодо потрібного рівня довіри (див. НД ТЗІ 2.5-003-99).

7.34 Якість документованості експлуатаційного середовища оцінюваної АТС вважається недостатньою, якщо в розпорядження Експерта на період оціночних робіт була надана не вся необхідна інформація, або якщо в наданих матеріалах є невідповідність нормуючим специфікаціям, які Заявник в обговорені терміни не зумів усунути.

7.35 Четверта група довірчих критеріїв пов'язана з одержанням гарантій того, що захищеність інформації у середовищах поставки, конфігурування, введення в дію і експлуатації оцінюваної АТС належним чином забезпечена.

У НД ТЗІ 2.5-003-99 наводяться специфікації рівнів довіри до середовищ поставки, конфігурування, введення в дію і експлуатації АТС, тобто визначаються вимоги до експлуатаційного середовища, які необхідно виконати, щоб мати можливість формального віднесення оцінюваної системи до одного із шести нормованих рівнів довіри.

7.36 Вихідними необхідними даними для оцінки захищеності інформації в експлуатаційному середовищі оцінюваної АТС є:

- матеріали з описом реалізованих гарантій безпеки середовища експлуатаційного персоналу;
- матеріали з описом реалізованих гарантій фізичної захищеності експлуатаційного середовища оцінюваної АТС;

- матеріали з описом реалізованих гарантій стандартизації експлуатаційного середовища оцінюваної АТС;

- матеріали з описом реалізованих гарантій якості документації на середовище експлуатації оцінюваної АТС;

- відомість поставленої конфігурації програмно-технічних засобів, яка ідентифікує комплект поставки оцінюваної АТС, і номер версії поставленого програмного забезпечення (комплектність оцінюваної АТС повинна бути відображена у технічних умовах або у відповідному документі на поставку);

- відомість поточної конфігурації (у випадку зроблених змін у поставленій конфігурації), яка ідентифікує склад АТС і програмного забезпечення до неї на момент оцінки.

7.37 Вище називані дані Заявник надає у розпорядження Організатора експертизи.

Зміст і форма наданих матеріалів залежить від очікуваного рівня довірчої оцінки коректності і визначається у специфікаціях згідно з НД ТЗІ 2.5-002-99 і НД ТЗІ 2.5-003-99.

7.38 У процесі оцінки захищеності інформації у експлуатаційному середовищі оцінюваної АТС аналізується шість аспектів:

- гарантії безпеки середовища експлуатаційного персоналу АТС (аспект 2.4.1);

- гарантії фізичної захищеності середовища експлуатації АТС (аспект 2.4.2);

- гарантії стандартизації середовища експлуатації АТС (аспект 2.4.3);

- гарантії якості документації на середовище експлуатації АТС (аспект 2.4.4);

- вимоги до поставки і конфігурування (аспект 2.4.5);

- вимоги до введення в дію і експлуатації (аспект 2.4.6).

7.39 Задача Експерта в процесі оцінки захищеності експлуатаційного середовища оцінюваної АТС полягає у послідовному перегляді дотримання вимог і умов, що специфіковані у НД ТЗІ 2.5-002-99 і НД ТЗІ 2.5-003-99.

7.40 Якість захищеності експлуатаційного середовища АТС вважається достатньою, якщо надані матеріали відповідають специфікаціям гарантій захисту і довірчих оцінок для потрібного рівня (див. НД ТЗІ 2.5-002-99 і НД ТЗІ 2.5-003-99).

7.41 Якість захищеності експлуатаційного середовища АТС вважається недостатньою, якщо у розпорядження Експерта на період оціночних робіт була надана не вся необхідна інформація, або якщо в наданих матеріалах є невідповідність нормованим специфікаціям, які Заявник в обговорені терміни не зумів усунути.

8 Порядок подання результатів оцінки захищеності інформації на АТС

8.1 Відповідно до вимог, які викладені в цьому документі, оцінці підлягає:

- коректність реалізації системи ТЗІ на оцінюваній АТС;
- рівень довіри до висновку про коректність реалізації системи ТЗІ на оцінюваній АТС.

Оцінка коректності реалізації системи ТЗІ виконується згідно критеріїв дієвості, викладеним у розділі 6.

Оцінка рівня довіри до коректності реалізації системи ТЗІ виконується згідно довірчих критеріїв, викладеним у НД ТЗІ 2.5-003-99.

8.2 АТС, система ТЗІ на якій відповідає всім критеріям дієвості і відповідає всім вимогам, викладеним у критеріях довіри для очікуваного оціночного рівня, повинна бути визнана як та, що успішно витримала випробування.

У цьому випадку оцінювана АТС одержує підтвердження того, що реалізована на ній система ТЗІ є коректною з рівнем довіри до коректності, що відповідає зазначеному у заявочних документах.

8.3 Якщо в процесі оціночних робіт з'ясовується, що який-небудь аспект оціночного рівня не виконується, наприклад через відсутність необхідної інформації або внаслідок того, що реальна характеристика оцінюваного об'єкта не відповідає специфікованим вимогам, і в заздалегідь обумовлені терміни Заявник не надав докази усунення поміченої недоробки, то об'єкт оцінки має бути відсторонений від оцінювання або одержати оцінку Е0.

8.4 Якщо рівень довіри до коректності реалізації системи ТЗІ на оцінюваній АТС визначений як Е0, то отримані оцінки стійкості механізмів захисту вважаються недійсними через брак довіри до оцінюваного об'єкту.

8.5 Оцінка стійкості реалізованих механізмів захисту одержує підтвердження тільки тоді, коли рівень довіри до коректності системи буде визнаний вище за рівень Е0. Градація рівнів стійкості механізмів захисту може бути тільки: базовий (низький), середній або високий.

8.6 Якщо аналіз "слабких місць" на оцінюваному об'єкті дав позитивний результат, але певний аспект оціночного рівня не виконується, то Заявнику може бути запропоновано виконати оціночні роботи відносно більш низького оціночного рівня. У випадку згоди Заявника з пропозицією щодо оцінки АТС на більш низькому рівні повторне виконання вже проведених оціночних робіт не проводиться.

8.7 Якщо в процесі оціночних робіт виявиться незафіксоване у наданих документах "слабке місце" й у заздалегідь обумовлені терміни Заявник не надав докази нейтралізації виявленого "слабкого місця", то об'єкт оцінки має бути відсторонений від оцінювання або одержати оцінку Е0.

8.8 За результатами оцінки Експерт дає Заявнику звіт, у якому вказується результат оцінки.

8.9 У випадку позитивного висновку Експертом і Заявником спільно готуються відповідні документи для подання в Уповноважений Орган із метою одержання формального юридично дієвого документа, що підтверджує коректність структури системи ТЗІ на оцінюваній АТС із рівнем довіри, який відповідає заявленому нормованому рівню довіри.

Переліки документів, що надаються в експертний орган для рівнів Е1-Е3, містяться у додатках до цього документу .

8.10 У випадку негативного висновку в звіті докладно і конкретно з посиланнями на відповідні НД наводяться аргументи і пояснюються причини, що спонукали Експерта зробити висновок про невідповідність результатів оцінки очікуваному рівневі.

8.11 У документі, що фіксує результат оцінки, вказується:

- структура системи ТЗІ на оцінюваній АТС (у вигляді визначеної множини функціональних послуг захисту із реалізованими рівнями стійкості механізмів захисту), коректність якої підтверджується;
- підтверджене значення рівня довіри (у межах від Е1 до Е6) до коректності структури системи ТЗІ, що реалізована на оцінюваній АТС.

Додаток А
(обов'язковий)

Перелік документів, що надаються в експертний орган для проведення експертизи щодо коректності реалізації систем захисту інформації на АТС із рівнем довіри Е1

А.1 Документи, що надаються Заявником оцінювальних робіт в Експертний орган:

- заява;
- стисла характеристика АТС (її паспорт або формуляр);
- перелік реалізованих ФПЗ;
- перелік реалізованих засобів та механізмів захисту;
- склад оцінюваної конфігурації програмно-технічних засобів АТС.

А.2 Документи, що надаються Організатором експертизи у Експертний орган:

- склад оцінюваної конфігурації програмно-технічних засобів АТС на момент початку оцінювальних робіт;
- програми та методики оцінювальних випробувань (зокрема, тестування) рівня Е1;
- протоколи оцінювальних випробувань (тестування) рівня Е1;
- експертні висновки усіх Експертів;
- узагальнений експертний висновок Організатора експертизи.

А.3 Документи, що надаються Експертами Організатору експертизи:

- програми та методики оцінювальних випробувань (тестування) рівня Е1;
- протоколи оцінювальних випробувань (тестування) рівня Е1;
- експертні висновки.

Додаток Б
(обов'язковий)

Перелік документів, що надаються в експертний орган для проведення експертизи щодо коректності реалізації системи захисту інформації на АТС із рівнем довіри Е2

Б.1 Документи, що надаються Заявником оцінювальних робіт в Експертний орган:

- заява;
- експлуатаційна документація на оцінювану АТС (у тому числі, формуляр, паспорт, інструкція з експлуатації та технічного обслуговування);
- стисла характеристика середовищ функціонування АТС - технологічного, інформаційного, користувачів та потенційних порушників;
- перелік суттєвих загроз для інформації;
- перелік реалізованих ФПЗ;
- перелік реалізованих засобів та механізмів захисту інформації;
- склад оцінюваної конфігурації програмно-технічних засобів АТС;
- стислий опис результатів аналізу експлуатаційної документації на функціональну повноту моделі захисту та КЗМЗ;
- програма та методика оцінювальних випробувань реалізованого КЗМЗ на рівні довіри Е2;
- протокол оцінювальних випробувань (зокрема, тестування) АТС на повноту та коректність надаваних ФПЗ і реалізованих механізмів захисту на рівні довіри Е2;
- програма та методика вимірювань характеристик технологічного середовища функціонування захищеної АТС;
- результати вимірювань параметрів ПЕМВН уздовж периметрів передбачуваних або реально визначених контрольованих зон;
- результати вимірювань побічних акустоелектричних перетворень в абонентських лініях зв'язку;
- перелік відомих "слабких місць" та "виломів" у системі ТЗІ, визначених на рівні довіри Е2, та заходів щодо їхнього знешкодження;
- перелік здійснених або здійснюваних гарантій захищеності експлуатаційного середовища АТС.

Б.2 Документи, що надаються Організатором експертизи в Експертний орган:

- склад оцінюваної конфігурації програмно-технічних засобів АТС на момент початку оцінювальних робіт;
- протокол оцінювання коректності моделі захисту та КЗМЗ на АТС;
- протокол випробувань (тестування) ФПЗ та КЗМЗ на АТС;
- протокол перевірки дієвості захисту від ПЕМВН та побічних акусто-електричних перетворень;
- перелік організаційно-технічних заходів щодо забезпечення ТЗІ;
- узагальнений експертний висновок Організатора експертизи.

Б.3 Документи, що надаються Експертом Організатору експертизи:

- протоколи виконаних аналізів та оцінювальних випробувань (тестування);
- експертні висновки.

Додаток В
(обов'язковий)

Перелік документів, що надаються в експертний орган для проведення експертизи щодо коректності реалізації системи захисту інформації на АТС із рівнем довіри Е3

В.1 Документи, що надаються Заявником оцінювальних робіт в Експертний орган:

- заява;
- експлуатаційна документація на оцінювану АТС (включаючи паспорт виробу, керівництво з експлуатації та технічного обслуговування, керівництво із застосування і т. ін.);
- документація рівня технічного проекту оцінюваної АТС і системи ТЗІ для неї у обсязі, визначеному вимогами НД ТЗІ 3.7-002-99 і НД ТЗІ 2.5-003-99;
- документація рівня робочого проекту оцінюваної АТС та системи ТЗІ для неї у обсязі, що визначений вимогами НД ТЗІ 3.7-002-99 і НД ТЗІ 2.5-003-99;
- документація з описом технологічних середовищ створення та експлуатації оцінюваної АТС та системи ТЗІ для неї в обсязі, що визначений вимогами НД ТЗІ 2.5-002-99;
- технічні умови (ТУ) на оцінювану АТС або для іноземних виробів - документ на поставку оцінюваної АТС рівня ТУ;
- склад оцінюваної конфігурації програмно-технічних засобів АТС;
- неформальний опис профілю технологічного середовища функціонування АТС;
- неформальний опис профілю середовища користувачів (типового, передбачуваного або реального);
- неформальний опис профілю інформаційного середовища експлуатації АТС (типового, передбачуваного або реального);
- неформальний опис профілю середовища потенційних порушників на етапі експлуатації АТС (типового, передбачуваного або реального);
- неформальний аналіз ризиків щодо можливих проявів загроз для інформації у передбачуваних або реальних умовах експлуатації АТС;
- перелік ймовірних загроз для інформації, які Заявник вважає суттєвими, з неформальною оцінкою гранично припустимих втрат від їх можливих реалізацій;
- перелік неформальних специфікацій ФПЗ, що занесені до бази захисту АТС;
- перелік неформальних специфікацій засобів та механізмів захисту інформації, що занесені до бази захисту АТС;
- неформальний аналіз (на рівні детальних пояснень та обгрунтувань) функціональної достатності та функціональної надмірності моделі захисту інформаційних ресурсів АТС;
- неформальний аналіз (на рівні детальних пояснень та обгрунтувань) функціональної достатності і функціональної надмірності КЗМЗ;
- неформальний аналіз (на рівні детальних пояснень і обгрунтувань) відомих "слабких місць" і "виломів" у проекті системи ТЗІ на оцінюваній АТС та ефективності заходів щодо їх знешкодження;
- результати вимірювань параметрів та аналізу структури сигналів у абонентських (як аналогових, так і цифрових) лініях зв'язку АТС;

- значення параметрів ПЕМВН уздовж периметрів передбачуваних (у разі сертифікації) або реально визначених (у разі атестації) контрольованих зон, усередині яких розміщені елементи оцінюваної АТС, та оцінки дієвості здійснюваних заходів захисту;

- результати вимірювань параметрів сигналів, утворених унаслідок побічних акусто-електричних перетворень, в абонентських (як аналогових, так та цифрових) лініях зв'язку та в термінальних лініях підсистеми керування АТС. Неформальний аналіз дієвості здійснюваних заходів захисту щодо нейтралізації загроз з боку каналів побічних акусто-електричних перетворень;

- методики, програми та протоколи приймально-здавальних випробувань (тестування) оцінюваної АТС на повноту і коректність виконуваних функцій і послуг (у т.ч., ФПЗ) відповідно до штатної документації (зокрема, до технічних умов);

- протоколи випробувань КЗМЗ на коректність реалізації ФПЗ згідно з нормованими специфікаціями;

- неформальний аналіз (на рівні детальних пояснень та обгрунтувань) надійності та живучості оцінюваної АТС;

- неформальний аналіз (на рівні детальних пояснень і обгрунтувань) відомих "слабких місць" і "виломів" у системі ТЗІ на АТС і ефективності заходів щодо їх знешкодження;

- перелік здійснених гарантій безпеки середовища творців оцінюваної АТС та системи ТЗІ для неї;

- перелік здійснених гарантій забезпечення конфіденційності та цілісності інформаційних ресурсів у середовищі створення АТС та системи ТЗІ для неї;

- перелік здійснених гарантій забезпечення спостережності та керованості середовища створення АТС і системи ТЗІ для неї;

- перелік здійснених або здійснюваних гарантій безпеки експлуатаційного персоналу АТС;

- перелік здійснених або здійснюваних гарантій захищеності експлуатаційного середовища АТС;

- перелік здійснених або здійснюваних гарантій стандартизації середовищ створення та експлуатації АТС;

- неформальний аналіз (звіт) здійснених або здійснюваних заходів на оцінюваній АТС щодо утримання та утилізації носіїв інформації ;

- перелік здійснених гарантій щодо якості експлуатаційної документації.

В.2 Документи, що надаються Організатором експертизи в Експертний орган:

- склад оцінюваної конфігурації програмно-технічних засобів АТС на момент початку оцінювальних робіт;

- протокол оцінювання коректності моделі захисту інформації на АТС;

- протокол оцінювання коректності КЗМЗ на АТС;

- протокол оцінювання ефективності (дієвості) бази захисту інформації на АТС (за результатами оцінки "слабких місць" та "виломів" у захисті);

- протокол перевірки дієвості захисту від ПЕМВН та побічних акусто-електричних перетворень;

- протоколи випробувань (тестування) системи ТЗІ на АТС;

- перелік прав доступу персонала до інформаційних ресурсів оцінюваної АТС;

- протокол перевірки реакції системи ТЗІ на нештатні дії абонентів та персоналу;

- протокол перевірки повноти, коректності та повторюваності тестів ФПЗ на припустимій множині вхідних даних;

- проект документу, що підтверджує результати оцінювання системи ТЗІ на АТС;

- перелік організаційно-технічних заходів щодо забезпечення ТЗІ на АТС;

- узагальнений експертний висновок Організатора експертизи.

В.3 Документи, що надаються Експертами Організатору експертизи:

- протоколи виконаних аналізів та оцінювальних випробувань (тестувань);

- експертні висновки.