НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Технічний захист інформації на програмно-керованих АТС загального користування

Порядок виконання робіт

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

Порядок виконання робіт

НД ТЗІ 2.7-001-99

ДСТСЗІ СБ України

Київ

Передмова

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

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

3 ВВЕДЕНО ВПЕРШЕ

Зміст

НД ТЗІ 2.7-001-99

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ПРОГРАМНО-КЕРОВАНИХ АТС ЗАГАЛЬНОГО КОРИСТУВАННЯ ПОРЯДОК ВИКОНАННЯ РОБІТ

Чинний від 1999-07-01

1 Галузь використання

Цей нормативний документ (НД) установлює вимоги до порядку виконання робіт з технічного захисту інформації (ТЗІ), що циркулює на програмно-керованих АТС загального користування, а також на установських (відомчих, корпоративних) АТС.

Положення НД поширюються на програмно-керовані АТС, а також на установські (відомчі, корпоративні) АТС (далі - АТС), у яких зберігається та циркулює інформація, що підлягає технічному захисту (див. ДСТУ 3396.0-96 і НД ТЗІ 1.1-001-99).

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, регіонального 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 правові акти і нормативні документи :

– Закон України "Про захист інформації в автоматизованих системах";

– Положення про технічний захист інформації в Україні. - Затверджено постановою Кабінету Міністрів України від 09 вересня 1994 р. за N 632;

– 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 - Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції;

– ГОСТ 2.106 96 - ЕСКД. Текстовые документы;

– ГОСТ 34.602-89 - Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

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

– НД ТЗІ 3.7-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова);

– НД ТЗІ 2.5-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;

– НД ТЗІ 2.5-002-99 - 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 - недосконаліть 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 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.

4 Загальні положення

4.1 Інформація, яка підлягає технічному захисту, у процесі функціонування АТС може зазнавати впливів загроз, внаслідок чого може виникнути її виток, порушення її цілісності або порушення доступності до неї з боку авторизованих користувачів (див., наприклад, Закон України "Про захист інформації у автоматизованих системах", "Положення про технічний захист інформації в Україні", Рекомендації Ради Європи №№ R (89)2, R (95)4 та ін.)

4.2 Спроможність системи ТЗІ протистояти впливам загроз визначає рівень захищеності інформаційних ресурсів АТС.

4.3 АТС, як правило, оснащуються штатними і, при необхідності, додатковими (позаштатними) засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності інформаційних ресурсів АТС.

4.4 Зміст і послідовність робіт з протидії загрозам та їх нейтралізації повинні відповідати вказаним у ДСТУ 3396.0-96 і ДСТУ 3396.1-96 етапам створення системи захисту інформації (див. рисунок 1) і полягати у:

- розробці технічного завдання на створення системи ТЗІ на АТС;

- розробці та реалізації техно-робочого проекту системи ТЗІ на АТС;

- оцінці захищеності інформаційних ресурсів АТС.

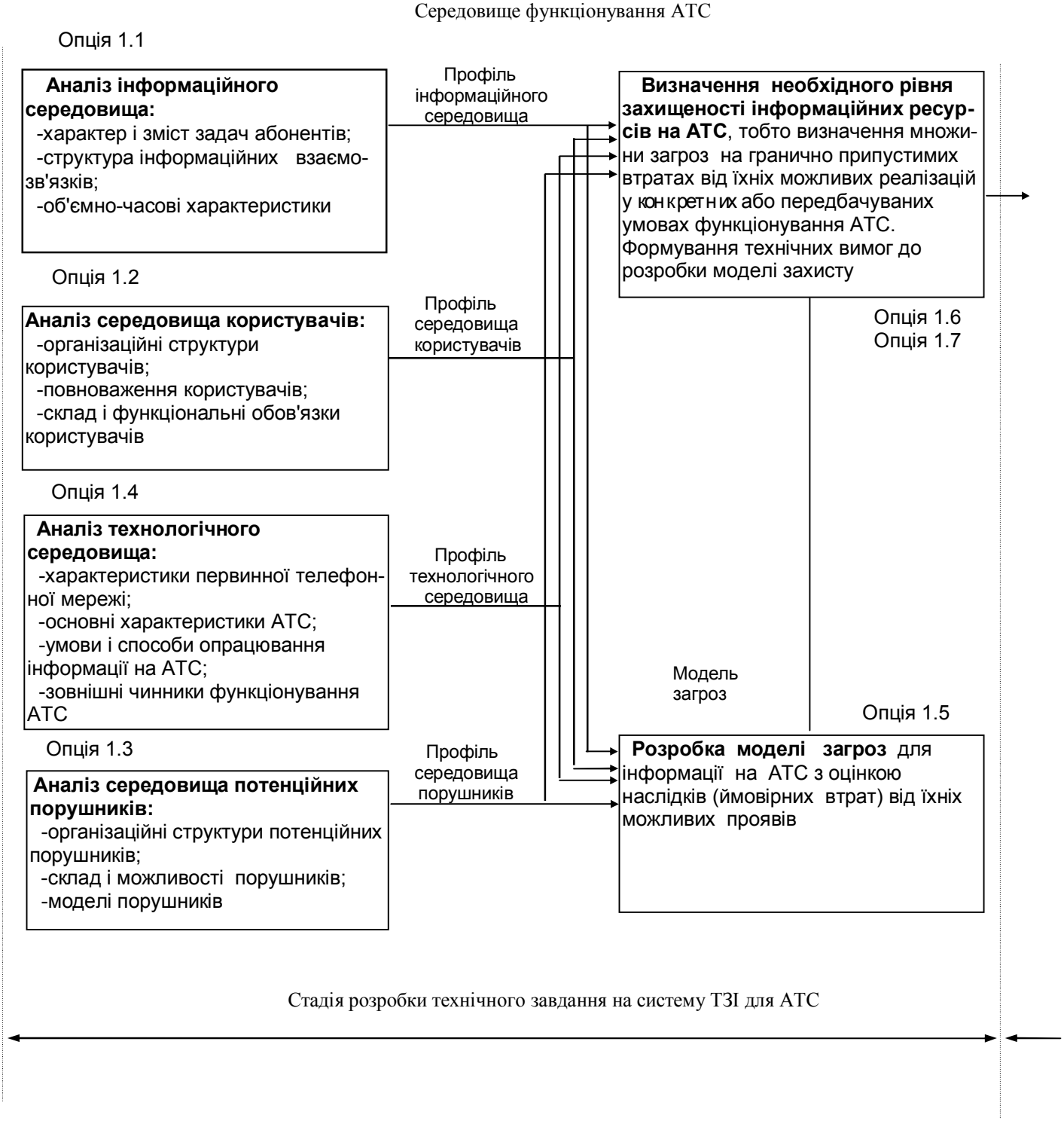


Рисунок 1- Схема організації робіт з ТЗІ на АТС

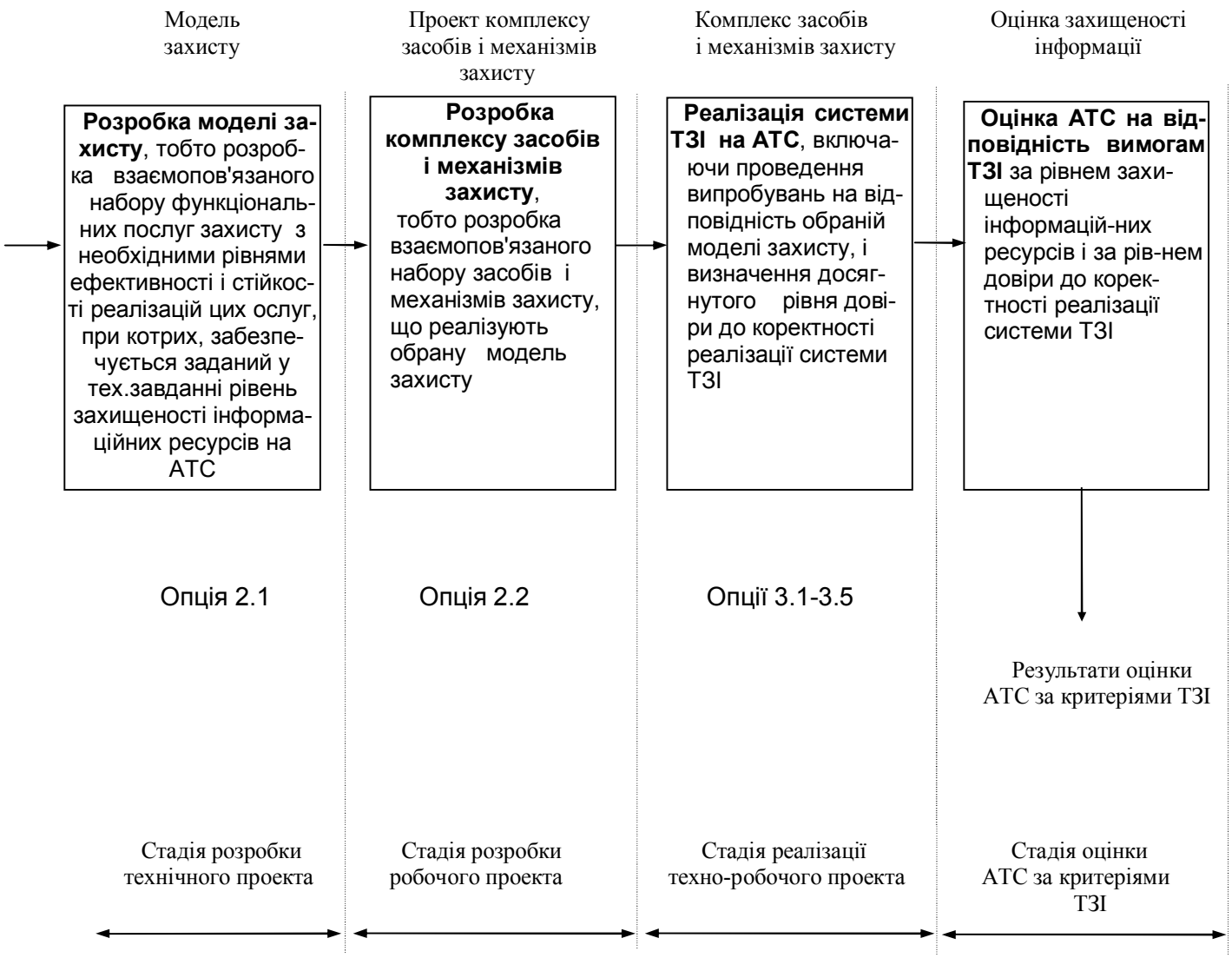


Рисунок 1 (продовження) - Схема організації робіт з ТЗІ на АТС

4.5 На початковому етапі для вперше створюваних автоматизованих систем (АС) (таких, наприклад, як інформаційні мережі з розподіленим керуванням і з розподіленим опрацюванням даних або таких, як системи комутації розмовних каналів зв'язку), у складі яких планується використання АТС, розроблюється підрозділ технічного завдання на АС за назвою "Вимоги до ТЗІ на АТС". Цей підрозділ включається до складу розділу технічного завдання (ТЗ), що відображає вимоги з ТЗІ на АС у цілому, і оформлюється згідно з ГОСТ 34.602-89. Крім того, в інших розділах ТЗ на АС, мають бути враховані вимоги з ТЗІ.

Для вже введених в експлуатацію АТС, але не атестованих за критеріями ТЗІ, ТЗ на систему ТЗІ на АТС розроблюється у вигляді окремого документу згідно з ГОСТ 34.602-89.

5 Розробка технічного завдання на створення системи ТЗІ на АТС

5.1 У процесі розробки ТЗ на систему ТЗІ на АТС:

– аналізуються інформаційні потоки через АТС, характер і зміст розв'язуваних її абонентами задач, рівень цінності (у т.ч., ступінь конфіденційності) інформації абонентів;

– оцінюються характеристики технологічного середовища експлуатації АТС, що підлягає захисту;

– створюються моделі порушників;

– виявляються дестабілізуючі чинники і загрози для інформаційних ресурсів;

– прогнозуються імовірності прояву загроз, потенційно можливі і припустимі втрати власників і абонентів АТС, що пов'язані з такими проявами;

– будується модель загроз;

– задаються вимоги до необхідного рівня захищеності інформаційних ресурсів на АТС.

5.2 Відповідно до принципу мінімальної достатності (див. НД ТЗІ 1.1-001-99) система захисту повинна бути спроектована таким чином, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для Замовника системи ТЗІ, і тільки в тій мірі, у котрій необхідно нейтралізувати (послабити, зменшити) наслідки прояву таких суттєвих загроз, для того щоб втрати від їхніх можливих реалізацій не перевищили гранично припустимих рівнів. Тому необхідний рівень захищеності інформації в технічному завданні визначається в термінах моделі загроз.

5.3 У процесі аналіза інформаційних потоків через АТС, характеру і змісту розв'язуваних її абонентами задач, як правило, керуються матеріалами, що викладені в підрозділах ТЗ на АС "Вимоги до функцій (задач), що виконуються системою" і "Вимоги до видів забезпечення", звертаючи особливу увагу на вимоги до інформаційного забезпечення (див. ГОСТ 34.602-89). Рівень цінності (у т.ч., ступінь конфіденційності) інформації, що циркулює на АТС, визначається Розроблювачем ТЗ і Замовником спільно.

5.4 Оцінка характеристик АТС і технологічного середовища її експлуатації, виявлення дестабілізуючих чинників і загроз для інформаційних ресурсів, оцінка імовірностей їхньої прояви і втрат, що пов'язані із можливими реалізаціями загроз, виконуються Розроблювачем на основі теоретичних і спеціальних експериментальних досліджень як самої АТС, так і середовища її функціонування.

5.5 Оцінка припустимих втрат і розробка вимог до необхідного рівня захищеності інформаційних ресурсів на АТС виконується Замовником ТЗ на основі наданих Розроблювачем ТЗ матеріалів, що містять аналіз задач абонентів АТС із позицій ТЗІ, аналіз загроз для інформаційних ресурсів і потенційних втрат, пов'язаних із їхніми можливими реалізаціями. Ці матеріали оформляються у вигляді ТЗ на розробку (створення) системи ТЗІ для АТС або, в окремих випадках, на розробку моделі захисту.

5.6 Зміст робіт із розробки ТЗ на систему ТЗІ наведений у розділі 8.

6 Розробка та реалізація техно-рабочего проекту системи ТЗІ на АТС

6.1 На стадії технічного проектування розроблюється модель захисту інформаційних ресурсів АТС (див. розділ 9).

Вибір моделі захисту здійснюється Розроблювачем технічного проекту і являє собою рішення задачі з мінімізації ресурсів захисту при забезпеченні наведеного в технічному завданні рівня захищеності інформаційних ресурсів АТС. У результаті рішення визначена сукупність ФПЗ, що пропонуються для реалізації в системі ТЗІ, оформлюється у вигляді технічних вимог до розробки КЗМЗ.

6.2 На стадії робочого проектування розроблюється КЗМЗ.

Для вперше створюваних АС, у складі котрих планується використання АТС, спочатку виконується вибір АТС з оглядом на реалізовані у ній ФПЗ таким чином, щоб мінімізувати вартість робіт із створення додаткових механізмів захисту (якщо в цьому виникає потреба).

У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у ТЗ рівень захищеності інформації. Іншими словами, необхідно вибрати таку АТС, штатні засоби захисту котрої (з урахуванням забезпечених гарантій захисту) за інших рівних умов найбільш повним чином реалізовували б отриману за результатами технічного проектування модель захисту.

6.3 Якщо АТС вже обрана, то виконується оцінка реалізованих у ній штатних ФПЗ на відповідність наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту.

6.4 Зміст робіт із розробки КЗМЗ відображений у розділі 9.

6.5 На стадії реалізації техно-робочого проекту здійснюється доробка і (або) дооснащення закупними виробами штатних програмно-технічних засобів АТС із тим, щоб таким чином створений КЗМЗ повною мірою містив у собі весь необхідний набір механізмів захисту, що був визначений у результаті робочого проектування. Необхідні додаткові (до штатних) механізми захисту (у тому числі і ті, що реалізовані в додаткових програмних і апаратних засобах захисту) включаються до складу поточної конфігурації АТС, що потребує захисту.

6.6 З метою спрощення процесу проектування системи ТЗІ і полегшення сприйняття результатів оцінки захищеності інформації на АТС за аналогією з Європейськими Критеріями безпеки (ITSEC) доцільно специфікувати перелік так називаних стандартних профілів вимог до захищеності інформації на АТС для різних типових галузей та умов її застосування. Наприклад, такі стандартні профілі, що відповідають класам безпеки "Жовтогарячої книги", стандартний профіль для банківських застосувань , що характеризується підвищеними вимогами і до цілісності і до конфіденційності інформації, стандартний профіль вимог для АТС загального користування з підвищеними вимогами до доступності і т. ін.

Кожний із стандартних профілів характеризується певним набором ФПЗ з визначеними рівнями стійкості їхніх реалізацій обраними механізмами захисту і визначеними рівнями гарантованості коректності як моделі захисту, так і системи ТЗІ в цілому.

6.7 У процесі проектування системи ТЗІ за основну (базову) сукупність ФПЗ зручно вибрати специфікований стандартний профіль вимог до АТС за критеріями ТЗІ, який найкраще відповідає прийнятій моделі захисту, щоб потім доповнити цю сукупність (якщо виникне потреба) відсутніми засобами і механізмами захисту з метою найбільш повного врахування нюансів конкретного застосування АТС. Тому у підсумковому документі з результатами оцінки доцільно вказати стандартний профіль вимог до захисту, взятий за основу для оцінюваної АТС, і оцінку якості реалізації сукупності ФПЗ, що використовуються на АТС як доповнення до послуг захисту вибраного стандартного профілю.

6.8 У процесі реалізації техно-робочого проекту:

– проводяться випробування створеного КЗМЗ на відповідність нормативним специфікаціям згідно з НД ТЗІ 2.5-001-99 і проектній документації;

– оцінюються, у тому числі й експериментальним шляхом, реальні характеристики середовища функціонування АТС після проведення заходів захисту;

– у необхідних випадках проводиться тестування захищеної АТС "на проникнення" (із метою пошуку нерозкритих "слабких місць" або "виломів" у захисті);

– оцінюється ефективність нейтралізації відомих "слабких місць" у захисті;

– оцінюється рівень довіри до коректності реалізованої системи ТЗІ.

6.9 Зміст робіт із реалізації техно-робочого проекту на систему ТЗІ відображений у розділі 10.

7 Оцінка захищеності інформації на АТС

7.1 На третьому етапі проведення робіт з ТЗІ виконується оцінка захищеності інформації на АТС незалежним експертним органом у конкретних або передбачуваних умовах її застосування.

7.2 Відповідно до розробленої методології оцінки захищеності інформації на АТС (див. НД ТЗІ 3.7-002-99) , гармонізованої з Європейськими Критеріями оцінки безпеки систем інформаційної техніки (Information Technology Security Evaluation Criteria,ITSEC), не ставиться задача віднесення рівня захищеності інформації в оцінюваній АТС до того або іншого класу і, отже, не висуваються з боку експертного органа апріорні вимоги до умов, у яких повинна працювати АТС.

Організація, що запитує послуги з оцінки ефективності ТЗІ на АТС, називана далі Заявником, описує умови, в яких повинна працювати АТС, можливі загрози безпеці її інформаційних ресурсів, визначає прийнятий для реалізації рівень захищеності АТС і представляє в оцінюючий орган документи (зокрема, ТЗ на систему ТЗІ, матеріали техно-робочого проекту системи ТЗІ, штатну документацію на АТС, програму, методику та протоколи приймально-здавальних випробувань системи ТЗІ і т.ін.), що підтверджують досягнутий рівень довіри до забезпечення гарантій і коректності реалізації функцій і механізмів захисту на АТС.

Задача оцінюючого органа - оцінити достатність і ефективність побудованої моделі захисту, а також повноту, коректність і ефективність реалізації КЗМЗ функціональних послуг захисту в описаних умовах функціонування АТС.

7.3 У процесі виконання оціночних робіт на основі матеріалів ТЗ на систему ТЗІ аналізуються умови, в яких повинна працювати АТС, оцінюється слушність вибору необхідного рівня захищеності інформаційних ресурсів, структурованого за видами загроз (тобто, оцінюється відповідність між припустимим на погляд Заявника рівнем втрат, пов'язаних із можливими реалізаціями конкретної множини загроз, і обраною моделлю захисту), і далі на основі матеріалів техно-робочого проекта на систему ТЗІ, технічної документації на АТС (особливо в частині опису комплекса засобів захисту), програми, методики і протоколів випробувань системи ТЗІ перевіряється ефективність і коректність реалізації обраної моделі захисту.

При цьому під ефективністю реалізації моделі розуміється:

- взаємна узгодженість відображених у моделі ФПЗ між собою;

- спроможність механізмів захисту, що реалізують на практиці задані у моделі ФПЗ, протистояти прямим атакам;

- неможливість практичного використання слабкостей в архітектурі АТС, тобто відсутність способів відключення, обходу, ушкодження й обману ФПЗ;

- неможливість практичного використання слабкостей в експлуатаційному середовищі АТС, тобто відсутність способів відключення, обходу, ушкодження й обману механізмів захисту експлуатаційного середовища;

- неможливість небезпечного конфігурування або використання АТС в умовах, коли засоби, що інформують персонал про перехід станції в небезпечний стан, відсутні або дають помилкові показання.

Під коректністю реалізації моделі захисту розуміється кон'юнкція слідуючих наведених нижче подій:

– проект КЗМЗ містить реалізації усіх без винятку ФПЗ, що включені у модель захисту;

– система ТЗІ, що реально створена на АТС, містить у собі всі без винятку засоби і механізми захисту, які відображені у проекті КЗМЗ;

– технічний проект системи ТЗІ містить опис ФПЗ, що відповідає специфікаціям НД ТЗІ 2.5-001-99;

– робочий проект системи ТЗІ містить опис механізмів захисту, що відповідає специфікаціям НД ТЗІ 2.5-001-99;

– механізми захисту, що включені в скад КЗМЗ, реально функціонують згідно з специфікаціями робочого проекту та специфікаціями НД ТЗІ 2.5-001-99 (за результатами випробувань системи ТЗІ, зокрема її тестування у процесі екплуатації).

7.4 Аналіз слабких місць робиться в контексті обраного Заявником необхідного рівня захищеності інформаційних ресурсів. Наприклад, можливо примиритися з наявністю таємних каналів передачі інформації, якщо відсутні вимоги до навмисних порушень конфіденційності. Слабкість конкретного захисного механізму стосовно певного виду загроз може не мати значення, якщо вона компенсується іншими засобами забезпечення безпеки.

7.5 Якщо в результаті виконання оціночних робіт зроблено висновок про те, що система ТЗІ, яка створена на АТС, що потребує захисту, реалізована коректно, то необхідно визначити ступінь впевненості в слушності такого висновку. Тут мається на увазі, що висновок про коректність 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.

7.6 У НД ТЗІ 2.5 - 003 - 98 визначаються сім можливих рівнів гарантованості коректності - від ЕО до Е6 (у порядку зростання вимог до глибини оцінки). Рівень ЕО означає відсутність гарантій коректності (це аналог класу Д з "Жовтогарячої книги"). На рівні Е1 аналізується лише загальна архітектура АТС - вся інша впевненість у коректності системи захисту повинна бути наслідком функціонального тестування. На рівні Е4 до аналізу залучаються вихідні тексти програм і схеми апаратури. На рівні Е6 потрібно мати формальний опис загальної архітектури АТС і обраної моделі політики безпеки. Відповідно до принципу безперервності захисту (див. НД ТЗІ 1.1 - 001 - 98) при перевірці коректності аналізується весь життєвий цикл АТС - від проектування до стадії промислової експлуатації включно.

7.7 Зміст робіт з оцінки ефективності ТЗІ на АТС відображений у розділі 11.

8 Порядок розробки вимог до системи ТЗІ на АТС

8.1 На стадії розробки ТЗ на систему ТЗІ на АТС (далі - ТЗ) виконуються такі види робіт, називані у цьому НД опціями (див. рисунок 1):

- аналіз інформаційного середовища, створеного або створюваного на базі АТС, що потребує захисту (опція 1.1);

- аналіз середовища користувачів АТС (опція 1.2);

- аналіз середовища потенційних порушників (опція 1.3);

- оцінка основних характеристик технологічного середовища функціонування штатних засобів АТС до проведення заходів захисту (опція 1.4);

- побудова моделі загроз для інформації на АТС, включаючи аналіз ризиків, що пов'язані із можливими реалізаціями загроз (опція 1.5);

- визначення необхідного рівня захищеності інформаційних ресурсів на АТС (опція 1.6);

- формування основних технічних вимог до розробки моделі захисту АТС, яке здійснюється на стадії технічного проектування (опція 1.7).

8.2 Розробка ТЗ являє собою двохетапний процес (див. рисунок 2).

8.3 Метою робіт, що здійснюються на першому етапі розробки ТЗ, є визначення необхідного рівня довіри до коректності створюваної системи ТЗІ, оскільки зміст і обсяг потрібних вихідних даних, виконуваних спеціальних досліджень і аналізів, рівень глибини (деталізації, формалізації) необхідних обгрунтувань однозначно залежать від потрібного рівня довіри до коректності системи захисту (див. НД ТЗІ 2.5 - 003 - 99) .

8.4 Змістом робіт, що здійснюються на першому етапі розробки ТЗ, є послідовне виконання опцій 1.1 - 1.6; при цьому зміст робіт в межах кожної із названих опцій викладений відповідно у 8.11 - 8.16 цього документу.

Аналіз передбачуваних середовищ функціонування АТС (див. опції1.1 - 1.4) виконується на якісному рівні в загальному вигляді, враховуються основні характеристики об'єктів й особливості взаємовідносин суб'єктів у досліджуваних середовищах.

На першому етапі розробки ТЗ визначаються:

– призначення АТС, що потребує захисту, і основні розв'язувані на її базі задачі;

– обсяги і ступінь важливості (цінності, у т.ч., конфіденційності) оброблюваної і транспортованої інформації;

– структура основних інформаційних взаємозв'язків;

– основні характеристики технологічного середовища експлуатації АТС, включаючи основні умови, режими і способи опрацювання і транспортування інформації;

– передбачувані межі зон, що потребують захисту;

– рівні інформативних випромінювань і навідів від побічних явищ;

– основні види загроз для інформації і технічні канали реалізації цих загроз;

– основні характеристики організаційних структур потенційних порушників.

У процесі захисту об'єктів особливої важливості вже на першому етапі розробки ТЗ може виникнути необхідність у проведенні спеціальних досліджень з метою експериментальної оцінки реальних характеристик передбачуваного середовища експлуатації АТС, якщо в результаті попереднього аналізу важко зробити висновки щодо передбачуваних значень параметрів досліджуваного середовища. У таких випадках спецдослідження виконуються відповідно до відомих спеціалізованих методик.

У рамках опцій 1.5 і 1.6 визначаються найбільш суттєві загрози в передбачуваних умовах застосування АТС, оцінюється співвідношення ресурсних можливостей захисту і потенційних порушників і з оглядом на цінність циркулюючої в АТС інформації приймається рішення щодо необхідного рівня довіри до коректності створюваної системи ТЗІ.

8.5 Вихідними даними для робіт, що виконуються в процесі розробки ТЗ, є:

- підрозділ "Вимоги до функцій (задач), що виконуються системою" і підрозділ "Вимоги до видів забезпечення" технічного завдання на вперше створювані і (або) вже створені автоматизовані системи, в складі яких використовується або планується використання АТС, що потребує захисту (див. ГОСТ 34.602-89);

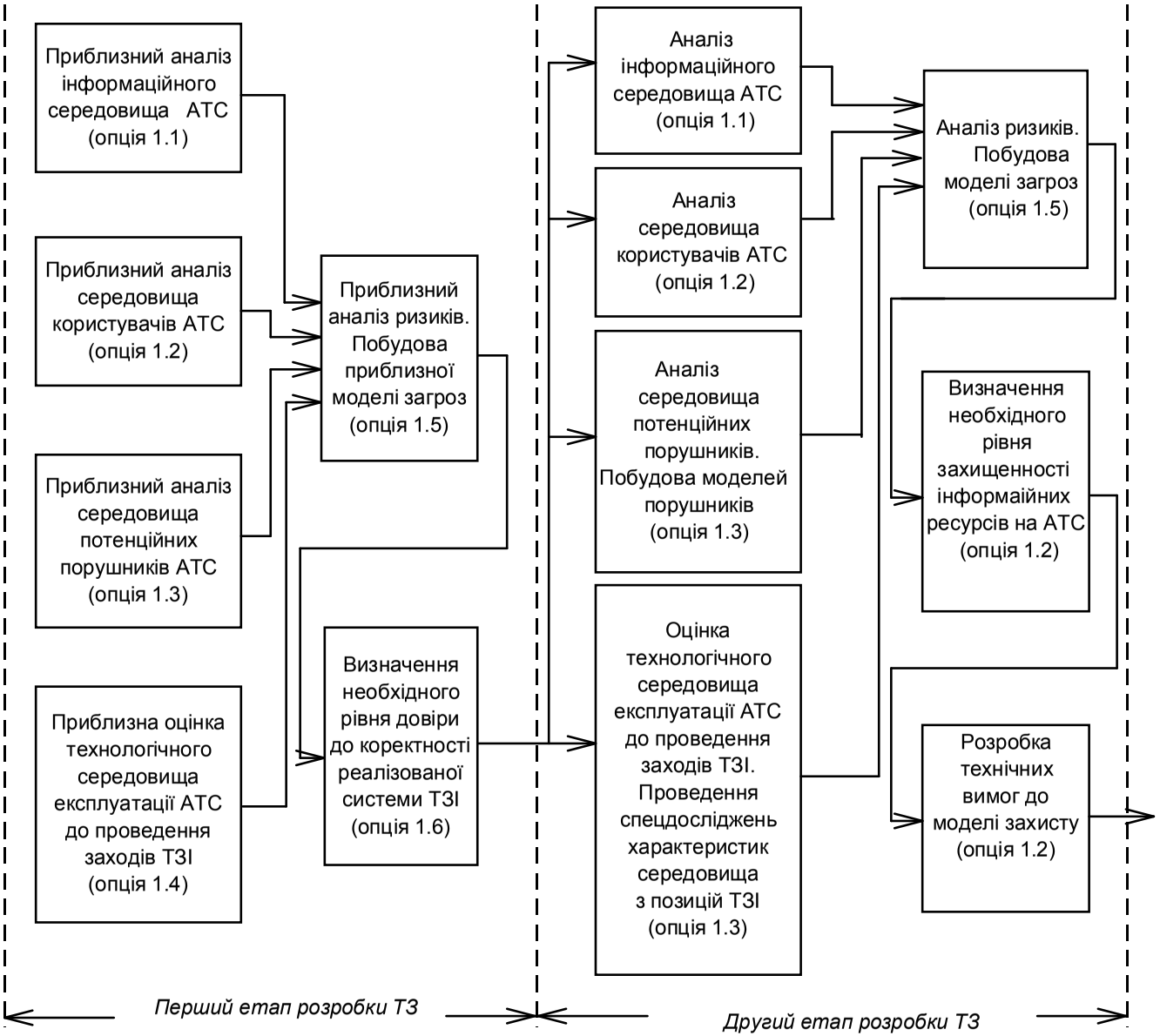


Рисунок 2 - Порядок розробки технічного завдання на систему ТЗІ для АТС

- організаційно-розпорядницька й експлуатаційна документація на фрагмент (ділянку) телефонної мережі, у складі якої використовується або планується використання АТС, що потребує захисту;

- документи, що містять описи організаційних структур користувачів (у т.ч., абонентів) АТС, що потребує захисту;

- документи, що містять описи організаційних структур потенційних порушників;

- комплект технічної документації, включений до складу поставленої конфігурації АТС;

- нормативні документи ТЗІ.

8.6 Результатом виконання першого етапу розробки ТЗ є обране значення необхідного рівня довіри до коректності створюваної системи ТЗІ.

8.7 Цілями робіт, що здійснюються на другому етапі розробки ТЗ, є:

– визначення необхідного рівня захищеності інформаційних ресурсів АТС, що потребує захисту;

– розробка основних технічних вимог до забезпечення ТЗІ з метою їх використання в процесі техно-робочого проектування системи захисту.

Необхідний рівень захищеності інформації визначається в термінах моделі загроз.

8.8 Змістом робіт, що здійснюються на другому етапі розробки ТЗ, є виконання опцій 1.1 - 1.7. Зміст робіт в межах кожної опції викладений відповідно у 8.11 - 8.17 цього документу. При цьому зміст і обсяг необхідних вихідних даних, запроваджуваних спеціальних досліджень і аналізів, рівень деталізації і формалізації виконуваних обгрунтувань однозначно залежать від необхідного рівня довіри до коректності системи ТЗІ.

8.9 За високих рівнів довірчих оцінок, починаючи з рівня Е4 і вище , необхідно розробити модель політики безпеки і, отже, повною мірою виконати аналіз середовищ функціонування АТС, створити моделі порушників, створити і проаналізувати модель загроз, виконати аналіз ризиків, обгрунтувати необхідний рівень захищеності інформаційних ресурсів АТС для конкретних або передбачуваних умов її експлуатації.

8.10 Результатами виконання другого етапу розробки ТЗ є:

– отриманий перелік суттєвих потенційних загроз для інформаційних ресурсів АТС із зазначеними гранично припустимими рівнями втрат від їхніх можливих реалізацій (тобто, визначений необхідний рівень захищеності інформаційних ресурсів АТС);

– основні технічні вимоги до розробки моделі захисту.

8.11 Змістом робіт, виконуваних у рамках опції 1.1

8.11.1 У процесі аналізу інформаційного середовища АТС досліджується:

- характер і зміст задач абонентів і персоналу станції;

- структура інформаційних взаємозв'язків;

- об'ємно-часові характеристики і ступінь важливості (цінності, у т.ч., конфіденційності) інформації, що циркулює в АТС.

8.11.2 Результатом робіт в опції 1.1 є опис профілю інформаційного середовища АТС, обумовленого як структурований набір можливо різнорідних визначень, показників і параметрів, що характеризує інформаційне середовище АТС із позицій ТЗІ.

8.12 Зміст робіт, виконуваних у рамках опції 1.2

8.12.1 У процесі аналізу середовища користувачів АТС досліджуються:

- організаційні структури користувачів (абонентів і персоналу станції);

- склад і функціональні обов'язки користувачів;

- повноваження користувачів.

8.12.2 Результат робіт в опції 1.2 - опис профілю середовища користувачів, який задається як структурований набір визначень, показників і параметрів, що характеризує середовище користувачів АТС із позицій ТЗІ.

8.13 Зміст робіт, виконуваних у рамках опції 1.3

8.13.1 У процесі аналізу технологічного середовища АТС досліджуються:

- основні характеристики АТС, що потребує захисту;

- характеристики первинної телефонної мережі;

- умови і способи опрацювання інформації штатними засобами АТС, що потребує захисту із позицій ТЗІ;

- зовнішні чинники середовища експлуатації АТС (у т.ч., спецдослідження) із позицій ТЗІ.

8.13.2 Результат робіт в опції 1.3 - опис профілю технологічного середовища, який задається як структурований набір визначень, показників і параметрів, що характеризує технологічне середовище експлуатації штатних засобів АТС.

8.14 Зміст робіт, виконуваних у рамках опції 1.4

8.14.1 У процесі аналізу середовища потенційних порушників досліджуються:

- організаційні структури потенційних порушників;

- склад і можливості потенційних порушників, що реалізують загрози для інформації на АТС;

- моделі потенційних порушників.

8.14.2 Результат робіт в опції 1.4 - опис профілю середовища потенційних порушників, що реалізують загрози для інформації через технічні канали, який задається як структурований набір моделей порушників.

8.15 Зміст робіт, виконуваних у рамках опції 1.5

8.15.1 У процесі аналізу середовища функціонування АТС виконується:

- аналіз ризиків, пов'язаних із можливими реалізаціями загроз, тобто оцінка частостей (імовірностей) проявів потенційних загроз і можливих рівнів втрат, пов'язаних із їхніми проявами, в умовах застосування штатних засобів АТС до проведення заходів захисту;

- побудова моделі загроз.

8.15.2 Результат робіт в опції 1.5 - побудована модель загроз для АТС, що потребує захисту.

8.16 Зміст робіт, виконуваних у рамках опції 1.6

8.16.1 За результатами побудови моделі загроз визначається необхідний рівень захищеності інформаційних ресурсів АТС.

8.16.2 Результат робіт в опції 1.6 - набір суттєвих загроз, стосовно котрих необхідно організувати протидію, з вказівкою гранично припустимих втрат від їхніх можливих реалізацій. Такі вказівки потрібні для визначення рівнів протидії суттєвим загрозам (див. аспект 2.1.2 у розділі 9).

8.17 Зміст робіт, виконуваних у рамках опції 1.7

8.17.1 На заключному етапі визначаються основні технічні вимоги до розробки моделі захисту АТС.

8.17.2 Результат робіт в опції 1.7 - основні технічні вимоги до розробки моделі захисту.

9 Порядок розробки техно-робочого проекту системи ТЗІ на АТС

9.1 У процесі техно-робочого проектування системи ТЗІ на АТС послідовно розроблюються (див. рисунок 1):

- технічний проект - модель захисту інформаційних ресурсів АТС (опція 2.1);

- робочий проект - проект комплексу засобів і механізмів захисту (опція 2.2).

9.2 Розробка технічного проекту

9.2.1 Метою робіт, що здійснюються в рамках опції 2.1, є створення моделі захисту, реалізація якої дозволить забезпечити заданий у ТЗ рівень захищеності інформаційних ресурсів АТС.

9.2.2 Порядок розробки технічного проекту системи ТЗІ показаний на рисунку 3.

9.2.3 Створення моделі захисту містить у собі проробку наступних аспектів у рамках опції 2.1:

– визначення множини функціональних послуг захисту, які у необхідній мірі протидіють загрозам, що включені в модель загроз (див. НД ТЗІ 2.5-001-99);

– визначення мінімально необхідних рівнів стійкості механізмів захисту, що реалізують послуги захисту з обраної множини функціональних послуг;

– оптимізація проекта моделі захисту за критеріями дієвості (див. НД ТЗІ 3.7-002-99);

– забезпечення функціональної достатності моделі захисту;

– усунення функціональної надмірності моделі захисту.

9.2.4 Старанність (глибина проробки, ступінь формалізації і деталізації) виконання технічного проекту однозначно залежить від потрібного рівня довіри до коректності розроблювальної системи ТЗІ і визначається специфікаціями, що наведені в НД ТЗІ 2.5 - 002 - 99 та НД ТЗІ 2.5-003-99.

9.2.5 Необхідними даними для проектування моделі захисту є основні технічні вимоги до її розробки, які розроблюються в рамках опції 1.7.

9.2.6 Результатом технічного проектування є модель захисту інформації на АТС.

9.3 Розробка робочого проекту КЗМЗ

9.3.1 Метою робіт, що здійснюються в рамках опції 2.2, є створення проекта КЗМЗ, що реалізує обрану модель захисту.

9.3.2 Порядок розробки робочого проекту показаний на рисунку 4.

9.3.3 Створення проекта КЗМЗ містить у собі проробку в рамках опції 2.2 таких аспектів:

– визначення множини засобів і механізмів захисту, які коректно реалізують функціональні послуги, що включені в модель захисту;

– проектування (вибір) засобів та механізмів захисту із заданими стійкостями (див. НД ТЗІ 1.1-001-99) від прямих впливів загроз;

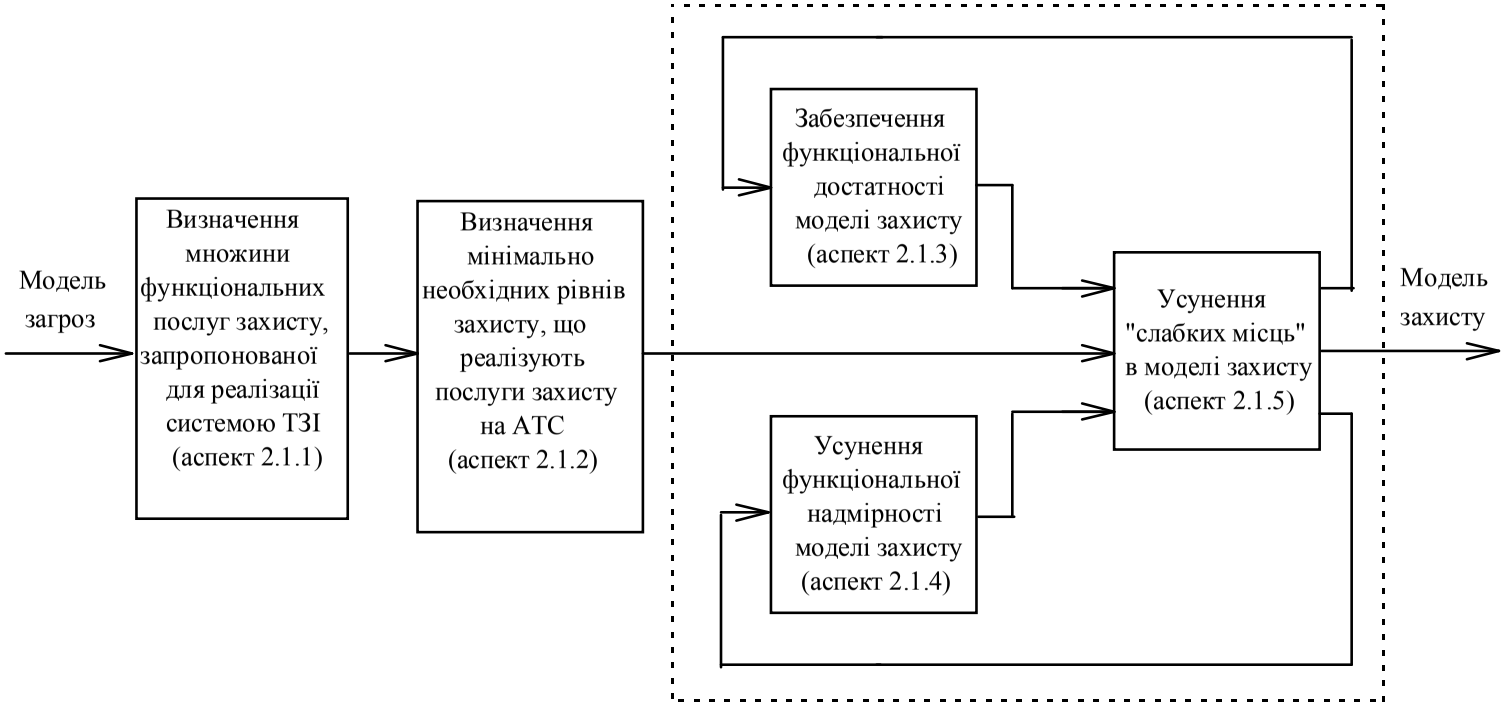


Рисунок 3 - Порядок розробки технічного проекта на систему ТЗІ для АТС

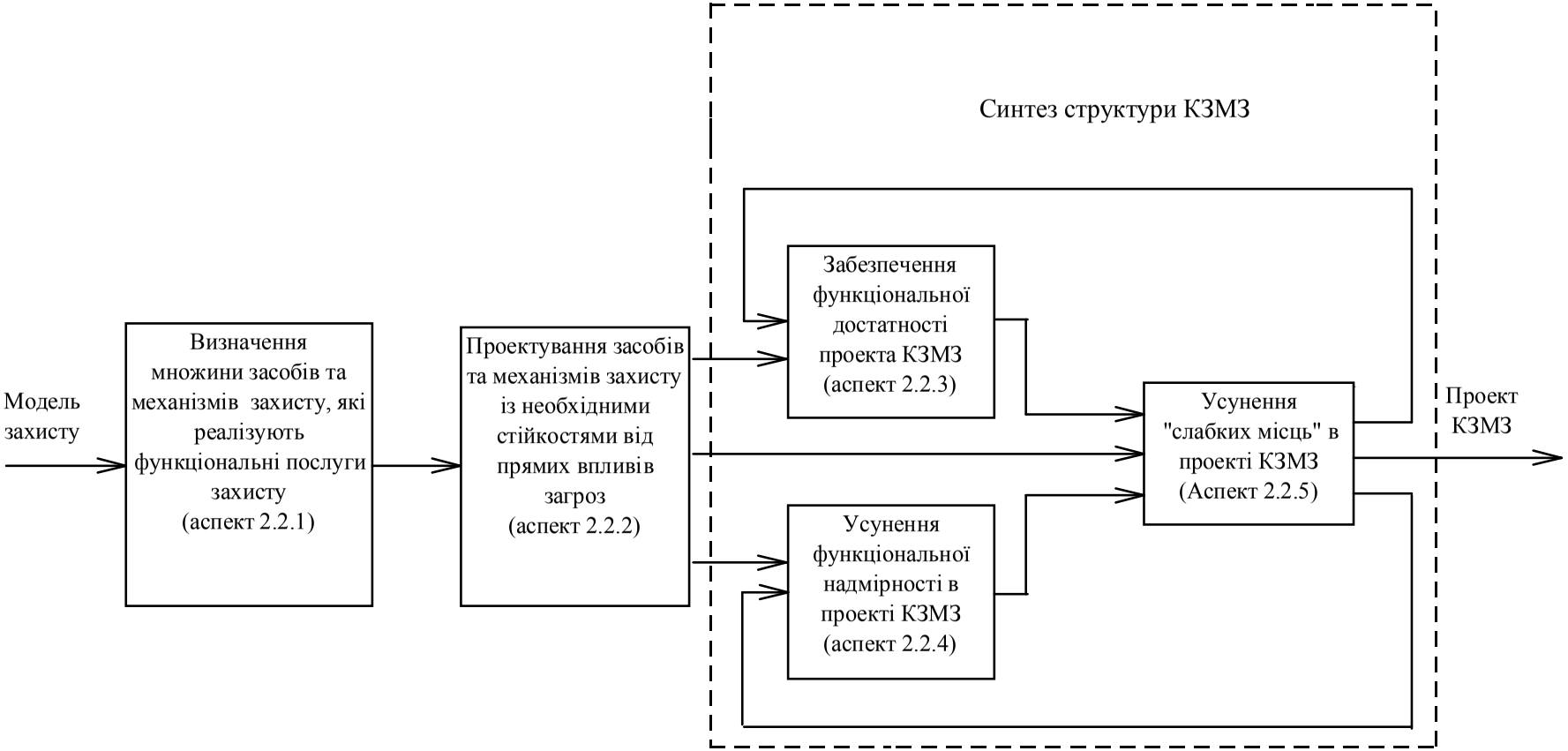


Рисунок 4 - Порядок розробки робочого проекта на систему ТЗІ для АТС

– усунення "слабких місць" у проекті КЗМЗ з урахуванням передбачуваних умов експлуатації комплексу;

– забезпечення функціональної достатності проекта КЗМЗ;

– усунення функціональної надмірності в проекті КЗМЗ.

9.3.4 Старанність (глибина проробки, рівень обгрунтувань) виконання робочого проекта однозначно залежить від потрібного рівня довіри до коректності розроблювальної системи ТЗІ і визначається специфікаціями, що наведені в НД ТЗІ 2.5 - 002 - 99 та НД ТЗІ 2.5 - 003 - 99.

9.3.5 Необхідними даними для проектування КЗМЗ є модель захисту, яка розроблена в рамках опції 2.1.

9.3.6 Результатом робочого проектування є проект КЗМЗ для АТС, що потребує захисту.

10 Порядок реалізації техно-робочого проекту системи ТЗІ на АТС

10.1 У процесі реалізації техно-робочого проекту системи ТЗІ на АТС виконуються такі види робіт (див.рисунок 5):

- програмна і (або) апаратна реалізація розробленого КЗМЗ (опція 3.1);

- випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації (опція 3.2);

- оцінка реальних характеристик технологічного середовища функціонування захищеної АТС після проведення заходів захисту (опція 3.3);

- оцінка ефективності нейтралізації "слабких місць" у захисті (опція 3.4);

- оцінка досягнутого рівня довіри до коректності реалізованої системи ТЗІ на АТС, що потребує захисту (опція 3.5).

Для виконання робіт у опціях 3.2 - 3.4 створюється програма та методика випробувань. Зміст програми та методики повинен відповідати ГОСТ 2.106-96.

10.2 Реалізація КЗМЗ

10.2.1 Метою робіт, що здійснюються в рамках опції 3.1, є реалізація КЗМЗ, який забезпечує наведений у ТЗ рівень захищеності інформаційних ресурсів АТС.

10.2.2 Змістом робіт, виконуваних у рамках опції 3.1, є програмна і (або) апаратна реалізація розробленого КЗМЗ.

Механізми захисту, які включені в проект КЗМЗ, але не реалізовані штатними засобами АТС, що потребує захисту, створюються на базі програмних і (або) апаратних засобів і включаються до складу поточної конфігурації АТС.

Деякі механізми захисту відповідно до проекту КЗМЗ реалізуються закупними засобами захисту, які повинні бути включені у відомість (перелік) закупних виробів системи ТЗІ.

Рівень захищеності інформації в середовищі виготовлення КЗМЗ однозначно залежить від потрібного рівня довіри до коректності створюваної системи ТЗІ і визначається специфікаціями, наведеними в НД ТЗІ 2.5 - 002 - 99, НД ТЗІ 2.5 - 003 - 99.

10.2.3 Результатом робіт в опції 3.1 є реалізований КЗМЗ.

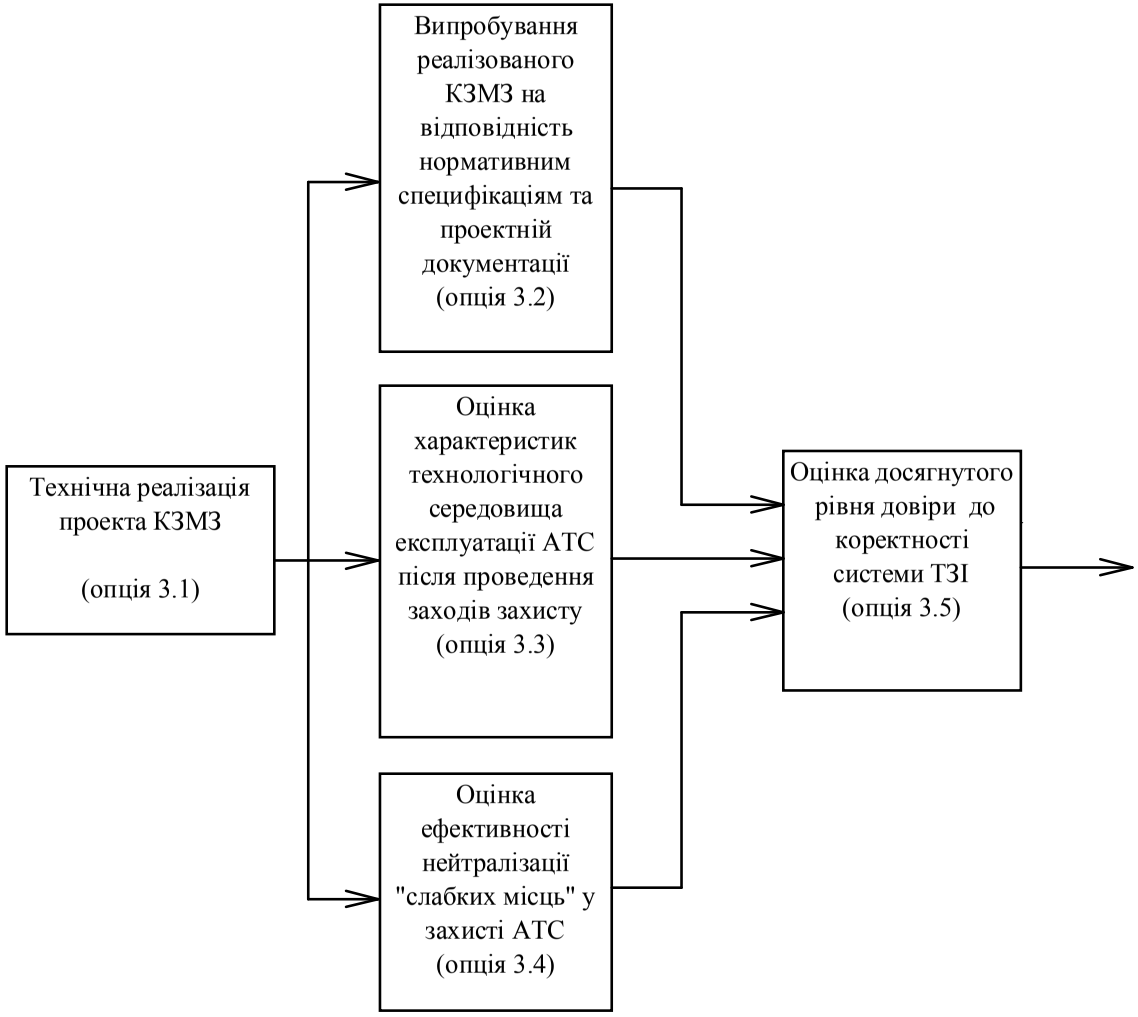


Рисунок 5 - Порядок реалізації техно-робочого проекта системи ТЗІ для АТС

10.3 Випробування КЗМЗ

10.3.1 Метою робіт, проведених у рамках опції 3.2, є одержання впевненості в тому, що реалізований КЗМЗ відповідає нормативним специфікаціям згідно з НД ТЗІ 2.5-002-99, НД ТЗІ 2.5-003-99 і проектній документації.

10.3.2 Змістом робіт, виконуваних у рамках опції 3.2, є випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації.

Обсяг і глибина запроваджуваних випробувань, а також повнота охоплення випробуваннями елементів АТС залежить від потрібного рівня довіри до коректності системи ТЗІ і визначається специфікаціями, що наведені в НД ТЗІ 2.5-003-99.

10.3.3 Результат випробувань - підтвердження потрібного рівня довіри до того, що реалізований КЗМЗ відповідає нормативним специфікаціям НД ТЗІ 2.5-003-99 і проектній документації.

10.4 Оцінка характеристик технологічного середовища функціонування захищеної АТС

10.4.1 Метою робіт, що здійснюються у рамках опції 3.3, є одержання впевненості в тому, що реальні характеристики технологічного середовища функціонування захищеної АТС після проведення заходів захисту знаходяться в припустимих діапазонах значень, що вказані у НД.

10.4.2 Змістом робіт, виконуваних у рамках опції 3.3, є визначення, у тому числі й експериментальним шляхом згідно із спеціалізованими методиками вимірів сигналів та полів від побічних явищ, реальних характеристик і параметрів середовища функціонування захищеної АТС і порівняння отриманих оцінок із нормованими припустимими значеннями відповідно до розробленої програми та методики проведення вимірювань.

Обсяг виконуваних спецдосліджень середовища, а також повнота охоплення дослідженнями елементів середовища залежить від потрібного рівня довіри до коректності системи ТЗІ і визначається специфікаціями, що наведені в НД ТЗІ 2.5-003-99.

10.4.3 Результат оцінки - підтвердження впевненості в тому, що реальні характеристики технологічного середовища функціонування захищеної АТС після проведення заходів захисту знаходяться в припустимих діапазонах значень.

10.5 Оцінка ефективності нейтралізації "слабких місць" у захисті

10.5.1 Метою робіт, здійснюваних у рамках опції 3.4, є одержання впевненості в тому, що "слабкі місця" в захисті інформаційних ресурсів АТС належною мірою задокументовані і нейтралізовані.

10.5.2 Змістом робіт, виконуваних у рамках опції 3.4, є:

– випробування захищеної АТС на можливість виявлення "слабких місць" у конструкції й у методах експлуатації (в тому числі, реалізація тестування "на проникнення");

– випробування реалізованого КЗМЗ на коректність і ефективність нейтралізації виявлених "слабких місць" і "виломів" у захисті.

Оцінка "слабких місць" у захисті повинна здійснюватися відповідно до розробленої програми та методики. Зміст програми та методики - згідно з ГОСТ 2.106-96.

Обсяг і глибина випробувань "слабких місць" у захисті однозначно залежать від потрібного рівня довіри до коректності системи ТЗІ і визначаються специфікаціями, що наведені в НД ТЗІ 2.5-003-99.

10.5.3 Результат випробувань "слабких місць" - підтвердження впевненості в тому, що в захисті АТС відсутні "виломи", а виявлені "слабкі місця" належним чином задокументовані і нейтралізовані.

10.6 Оцінка досягнутого рівня довіри до реалізованої системи захисту

10.6.1 Метою робіт, що здійснюються в рамках опції 3.5, є підтвердження наведеного в ТЗ рівня довіри до коректності реалізованої системи ТЗІ на АТС, що потребує захисту.

10.6.2 Змістом робіт, виконуваних у рамках опції 3.5, є оцінка рівня довіри до коректності реалізованої системи ТЗІ за методикою, викладеною в НД ТЗІ 3.7-002-99 .Ця методика базується на специфікаціях довірчих оцінок, визначених у НД ТЗІ 2.5-003-99.

10.6.3 Результат оціночних робіт в межах опції 3.5 - підтвердження того, що отримана оцінка рівня довіри відповідає очікуваному рівню, який наведений у ТЗ.

11 Порядок оцінки захищеності інформаційних ресурсів АТС

11.1 На етапі оцінки захищеності інформаційних ресурсів АТС послідовно виконуються такі види робіт (див. рисунок 6):

- перевірка коректності побудованої моделі загроз;

- перевірка коректності побудованої моделі захисту;

- перевірка коректності проекту КЗМЗ;

- перевірка коректності реалізації КЗМЗ;

- перевірка виконання нормативних вимог до конструкторської й експлуатаційної документації на систему ТЗІ для оцінюваної АТС відносно заявленого рівня довіри;

- перевірка дотримання нормативних гарантій забезпечення захищеності інформації в технологічних середовищах створення й експлуатації оцінюваної АТС, включаючи систему ТЗІ, відносно заявленого рівня довіри.

11.2 Цілями оцінки АТС за критеріями ТЗІ є:

- підтвердження ефективності і коректності розробленої і реалізованої на АТС системи ТЗІ;

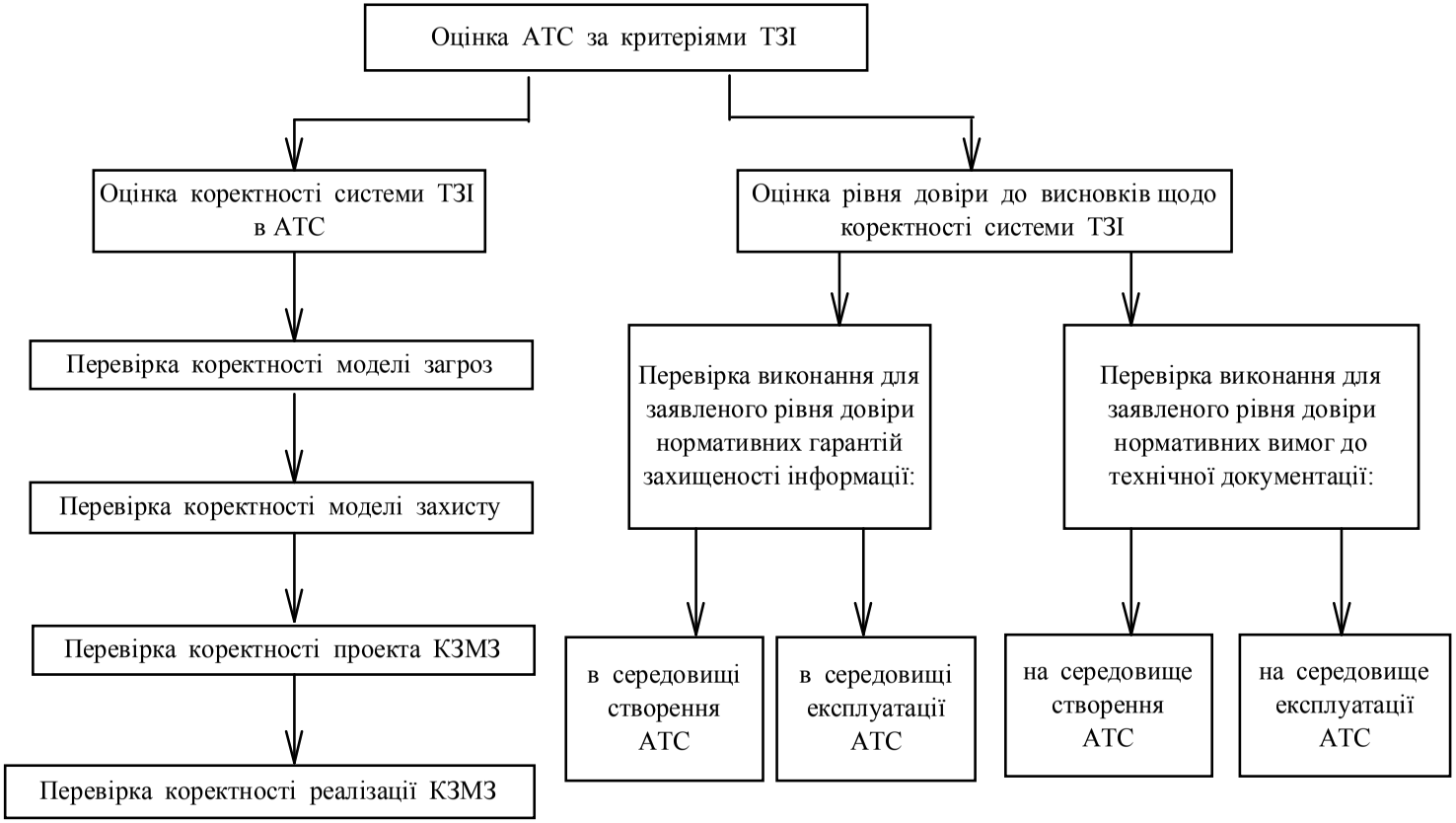
- підтвердження заявленого рівня довіри до висновку про коректність системи ТЗІ в оцінюваній АТС.

11.3 Процес оцінки АТС за критеріями ТЗІ регламентований базовою методикою оцінки ефективності захисту, викладеною в НД ТЗІ 2.3 - 001 - 99 . Ця методика ґрунтується на специфікаціях ФПЗ (див. НД ТЗІ 2.5 - 001 - 99), специфікаціях гарантій захищеності інформації (див. НД ТЗІ 2.5 - 002 - 99) і специфікаціях довірчих оцінок коректності реалізації захисту (див. НД ТЗІ 2.5 - 003 - 99).

Крім того, у процесі оціночних робіт використовуються окремі спеціалізовані методики оцінки якості ТЗІ від НСД, витоків та спеціальних впливів.

11.4 Ступінь впевненості в коректності створеної системи ТЗІ у вигляді заявленого до оцінки рівня довіри (будь-якого із шести градацій - від Е1 до Е6) і рівень захищеності інформаційних ресурсів у вигляді певної множини функцій безпеки, для яких зазначені рівні стійкості створених механізмів захисту, вказуються Заявником у процесі оформлення заявки на виконання оціночних робіт. Така заявка направляється на адресу уповноваженого державою експертного органа.

11.5 Процес оцінювальних робіт у випадку сертифікації АТС за критеріями ТЗІ регламентується нормативними документами УкрСЕПРО - зокрема, ДСТУ 3413-96.



Рисуок 6 - Порядок оцінки АТС за критеріями ТЗІ

11.6 Розглянувши заявку, експертний орган надає Заявнику поштові реквізити оцінювачів - незалежних від Заявника організацій (як правило, випробувальних лабораторій або центрів), що мають право і здатні виконувати роботи з оцінки захищеності інформаційних ресурсів АТС на тому рівні довіри до результатів оцінки, який влаштовує Замовника.

11.7 Далі, відповідно до правил, що регламентовані в ДСТУ 3413-96, укладається договір між Заявником, що виступає за Замовника, і Оцінювачем, що виступає за Виконавця, на проведення оціночних робіт із метою одержання позитивного або негативного висновку 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 перебуває на одному із нормованих рівнів, що зазначив Заявник у заявочних документах.

11.8 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 специфікаційним вимогам. У такому випадку Заявнику надається право в заздалегідь обумовлені строки усунути зауваження (наприклад, надати відсутню інформацію, виправити помилку, доробити елемент захисту і т. ін.). У протилежному випадку, оцінюваний об'єкт буде мати результат оцінки на рівні ЕО.

11.9 За результатами оцінки Оцінювач надає Заявнику звіт, в якому вказується результат оцінки.

11.10 У випадку негативного висновку в звіті докладно і конкретно з посиланнями на відповідні НД наводяться аргументи і пояснюються причини, що спонукали Оцінювача зробити вивід про невідповідність результатів оцінки до очікуваної цілі.

11.11 У випадку позитивного висновку Оцінювачем і Заявником спільно готуються відповідні документи (див. додатки до НД ТЗІ 3.2- 002-99) для подання в експертний орган із метою одержання формального юридично дієвого документа, що підтверджує коректність зазначеної в ньому структури системи ТЗІ на АТС із рівнем довіри, що відповідає зазначеному нормативному рівню довіри.

11.12 Таким чином, у названому вище документі вказується:

– структура створеної на АТС системи ТЗІ у вигляді множини функцій безпеки з реалізованими рівнями стійкості механізмів захисту, коректність якої підтверджується;

– підтверджене значення рівня довіри (у межах від Е1 до Е6) до коректності зазначеної в документі структури системи ТЗІ.

11.13 Для того, щоб оцінка була виконана ефективно і з мінімальними витратами, Оцінювач може співробітничати із Заявником і (або) Розроблювачем системи ТЗІ, проте Оцінювач повинний бути незалежним (не приймати участі у розробці системи ТЗІ для оцінюваної АТС).

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

11.15 Зміст і обсяг проведених у процесі оцінки експериментальних досліджень, перелік, зміст і форма необхідних для аналізу документів, рівень старанності (формалізації,

деталізації, строгості) обгрунтувань і доказів, наданих 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 НД ТЗІ 2.5 - 003 - 99.

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

11.17 У базовій методиці НД ТЗІ 2.3 - 001 - 99 для кожного оціночного рівня визначені вимоги до переліку, змісту і форми документів, що повинний передати Заявник у розпорядження Оцінювача, і, отже, заздалегідь їх підготувати ще до проведення оціночних робіт.

11.18 У процесі оцінювання за вищими рівнями довіри виникає необхідність у розробці і виготовлені спеціальних схем дослідження "слабких місць", глибоких тестів " на проникнення", моделюванні дій "хакерів", формального опису політики безпеки. Всю вище перераховану роботу повинний узяти на себе Заявник і відповідати за повноту і коректність її виконання. Оцінювач може взяти на себе роботу з перегляду наданих Заявником тестів, моделей, схем, аналізів, обґрунтувань і доказів, має право їх доповнювати й удосконалювати, досліджувати власними методами і засобами слабкі місця у захисті.

11.19 Для всіх оціночних рівнів, за винятком Е1, Оцінювач повинний переважно перепровіряти результати випробувань і аналізу, які Заявник надав у його розпорядження.

На оціночному рівні Е1 оцінка може робитися тільки за результатами аналізу документації користувача. Заявник у цьому випадку може і не давати результати випробувань створеної на АТС системи ТЗІ.