Зміст

НД ТЗІ 1.1-001-99

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ПРОГРАМНО-КЕРОВАНИХ АТС ЗАГАЛЬНОГО КОРИСТУВАННЯ ОСНОВНІ ПОЛОЖЕННЯ

Чинний від 1999-07-01

1 Галузь використання

Цей нормативний документ (НД) установлює об'єкт, ціль та основні організаційно-технічні положення технічного захисту інформації (ТЗІ) на АТС, що призначені для функціонування на проводових телефонних мережах загального користування та (або) на установських (відомчих, корпоративних) системах зв'язку.

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

Вимоги НД не поширюються на захист:

- міжстанційних каналів синхронізації, сигналізації та передачі абонентської інформації;

- від зловмисних дій авторизованих користувачів у межах наданих їм повноважень, що наносять збиток власникам інформаційних ресурсів;

- елементів АТС від екстремізму і вандалізму авторизованих користувачів;

- телефонної мережі від некоректного вмикання в її структуру вперше запроваджуваних АТС або АТС, що модернізуються.

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

Документ призначений для замовників, розроблювачів, виготовлювачів і постачальників АТС, операторів зв'язку національного, 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 НД ТЗІ використані посилання на такі нормативні документи :

- Концепція про технічний захист інформації в Україні. Затвердження Постановою Кабінету Міністрів України від 2.10.97р., № 1126;

– 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 проведення робіт;

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

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

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

– НД ТЗІ 2.5-002-99 - 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;

– НД ТЗІ 2.7-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

3 Визначення, позначення і скорочення

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

Крім того, вводяться або уточнюються стосовно до АТС 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.

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.

КАЗЛ - підсистема комутації абонентських і з'єднувальних ліній зв'язку на АТС.

ПРД - правила розмежування доступу.

СРД - система розмежування доступу.

4 Загальні положення

4.1 Об'єктом технічного захисту на програмно-керованих АТС, а також на установських (відомчих, корпоративних) АТС є конфіденційна, а також відкрита важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих АТС.

4.2 Метою ТЗІ на програмно-керованих АТС загального користування, а також на установських (відомчих, корпоративних) АТС є запобігання за допомогою інженерно-технічних заходів здійсненню загроз інформаційним ресурсам (далі - загроз для інформації) АТС.

4.3 Документ є методологічною базою нормативних і методичних документів, що спрямовані на розв'язання таких задач:

- розробка вимог щодо захисту інформації на АТС;

- створення захищених АТС ;

- створення систем і засобів ТЗІ на АТС;

- створення систем керування комплексами засобів ТЗІ на АТС;

- оцінка захищеності інформації на АТС;

- оцінка ефективності систем і засобів ТЗІ на АТС.

5 Основні принципи ТЗІ на АТС

5.1 Принцип легітимності захисту - ТЗІ на АТС (далі - захист АТС) повинен ґрунтуватися на положеннях і вимогах чинних в Україні нормативно-правових актів і нормативних документів щодо технічного захисту інформації, в тому числі на положеннях Концепції про технічний захист інформації в Україні, що затверджена постановою Кабінету Міністрів України від 2.10.97р., №1126.

5.2 Принцип комплексності захисту - захист АТС повинен забезпечуватися комплексом взаємопов'язаних програмно-технічних засобів і організаційних заходів.

5.3 Принцип безперервності захисту - захист АТС повинен забезпечуватися на всіх технологічних етапах опрацювання викликів і у всіх режимах функціонування і надання послуг, зокрема при проведенні ремонтних і регламентних робіт.

5.4 Принцип мінімальної достатності захисту - захист АТС повинен забезпечувати необхідний рівень захищеності при мінімальних витратах ресурсів.

5.5 Програмно-технічні засоби захисту не повинні істотно погіршувати основні характеристики АТС (пропускну спроможність, надійність, можливість зміни конфігурації АТС і т. ін.).

5.6 Невід'ємною частиною робіт з ТЗІ на АТС є оцінка ефективності засобів захисту, що здійснюється згідно з методиками, які враховують всю сукупність технічних характеристик оцінюваного об'єкта, включаючи технічні рішення і практичну реалізацію засобів захисту.

5.7 Захист АТС повинен передбачати створення систем керування комплексами засобів захисту, що дозволяють здійснити безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів АТС.

6 Структура програмно-керованих АТС із позицій ТЗІ

6.1 Структура програмно-керованої АТС, що відображена на рисунку 1, з позицій ТЗІ розподіляється на дві відносно незалежні підсистеми:

- підсистема керування станцією;

- підсистема комутації абонентських і з'єднувальних ліній зв'язку (КАЗЛ).

6.2 Підсистема керування станцією містить у собі:

– спеціалізовані пристрої керування, що реалізують принцип програмного керування і складаються, здебільшого, з процесорів, пристроїв внутрішньої і зовнішньої пам'яті, периферійних пристроїв, спеціалізованих модулів керування сигналізацією, опрацюванням викликів, наданням послуг і деяких інших програмно-апаратних компонентів, які є характерними для комп'ютерної техніки;

– термінали обслуговування, що під'єднані до пристроїв керування через канали технологічного обслуговування АТС і до підсистеми КАЗЛ - через канали інформаційного обслуговування абонентів.

6.3 Підсистема КАЗЛ містить у собі пристрої, що реалізують процеси комутації, мультиплексирування та концентрації абонентських і міжстанційних з'єднувальних ліній, а також компоненти устаткування абонентських ліній зв'язку - абонентські прикінцеві пристрої, фізичні лінії зв'язку, пристрої мультиплексирування абонентських ліній, станційні абонентські комплекти і т. ін.

На виходах підсистеми керування утворюються в реальному часі потоки технологічних сигналів, за допомогою яких має місце процес керування підсистемою КАЗЛ. З іншого боку, абонентські прикінцеві пристрої мають можливість обмінюватися керуючою

інформацією з підсистемою керування станцією через канали керування з'єднанням і замовленням послуг.

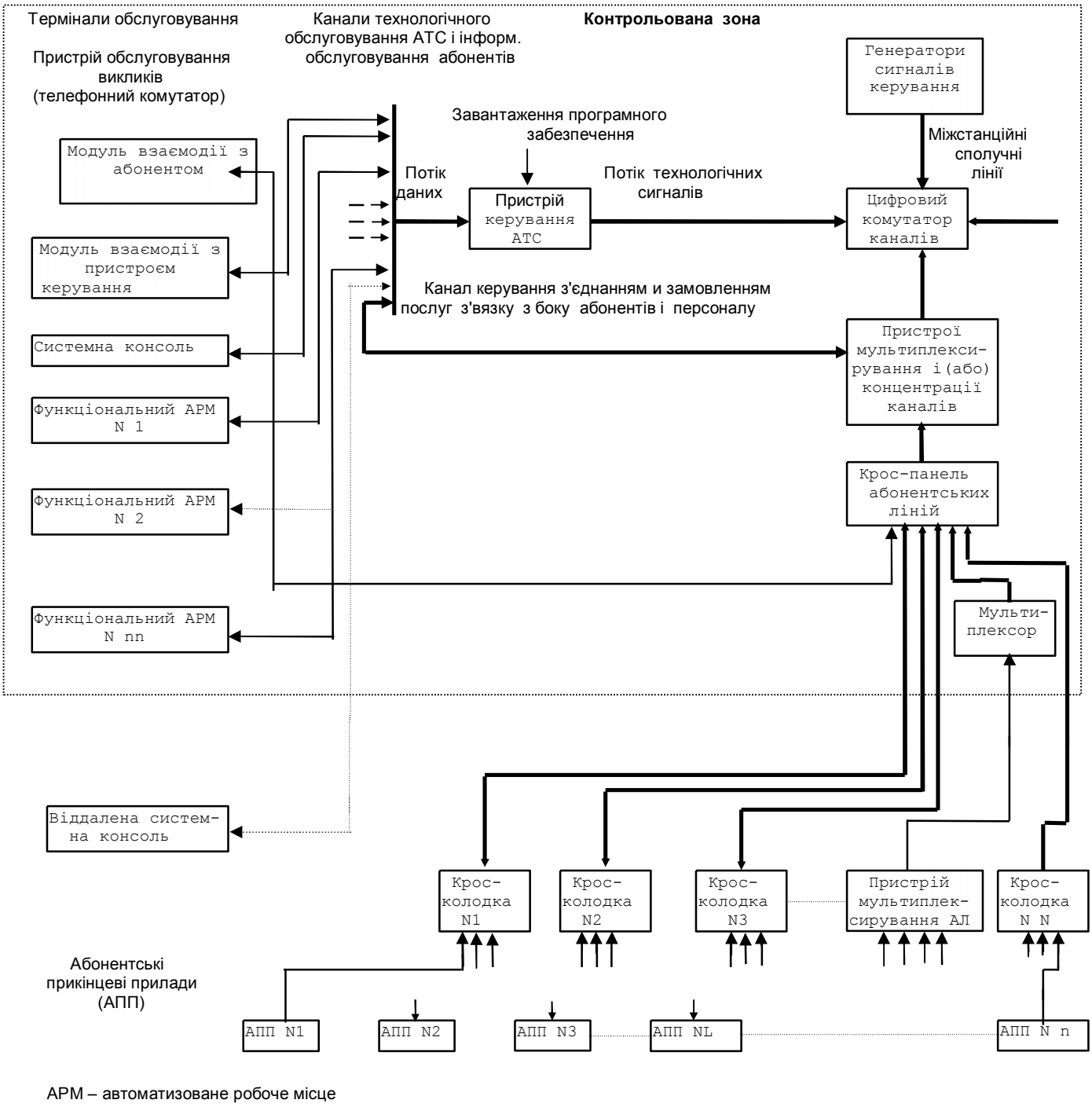
6.4 Незалежність вищезгаданих підсистем керування станцією і КАЗЛ розуміється в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми керування станцією, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, за передумовою відсутності механізмів реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ і, навпаки, - на підсистемі КАЗЛ з боку підсистеми керування станцією.

Коректність такої декомпозиції структури програмно-керованих АТС обумовлена прийнятими щодо них проектними рішеннями , що не передбачають:

- можливостей штатних впливів на підсистему керування станцією з боку абонентських прикінцевих пристроїв, за винятком можливості запуску абонентом задач із фіксованого набору, що реалізують заздалегідь передбачені функції замовлення абонентом додаткових видів послуг, які надаються станцією;

- можливостей штатних впливів на інформацію в розмовних трактах із боку підсистеми керування станцією, за винятком можливості штатних під'єднань до вже встановлених з'єднань (наприклад, із боку телефонного комутатора або абонентських прикінцевих пристроїв у режимі конференцзв'язків), однак з обов'язковим оповіщенням учасників розмови про всі додаткові підключення до їхніх розмовних трактів (зокрема, фоновими тональними сигналами).

6.5 Відносність незалежності вищезгаданих підсистем розуміється в тому сенсі, що за певних умов внаслідок помилок або некоректних (зокрема, зловмисних) дій, які були допущені на передексплуатаційних стадіях життєвого циклу АТС (наприклад, при установці програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності АТС, тим не менш, можливі реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ, і, навпаки, - на підсистемі КАЗЛ з боку підсистеми керування станцією. Тому для обгрунтування коректності розподілу структури АТС на дві вищезгадані підсистеми необхідно надати докази щодо коректності реалізації проекту АТС. Такі докази виконуються, як правило, на стадії розробки технічного проекту системи ТЗІ.



АРМ – автоматизоване робоче місце

Рисунок 1 - Структурна схема програмно-керованої АТС з позицій ТЗІ

7 Види загроз для інформації

7.1 У програмно-керованих АТС розрізняють такі види загроз для інформації:

- порушення конфіденційності (тобто, ознайомлення з інформацією обмеженого доступу неавторизованими особами);

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

- порушення доступності або відмова в обслуговуванні (тобто, позаштатні обмеження в реалізації авторизованими користувачами штатних процедур доступу до інформаційних ресурсів);

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

- несанкціоноване користування інформаційними ресурсами станції (зокрема, несанкціоноване користування послугами, що надаються станцією і т. ін.).

7.2 У цьому документі такий вид загроз як витік інформації (тобто, неконтрольоване поширення інформації, що веде до несанкціонованого її одержання) розглядається як окремий випадок прояву порушень конфіденційності.

7.3 У цьому документі такий вид загроз як блокування інформації (тобто, порушення можливості санкціонованого доступу до інформації) розглядається як окремий випадок прояву порушень доступності.

8 Шляхи реалізації загроз для інформації

8.1 Загрози для інформації на АТС можуть здійснюватися:

– шляхом НСД до інформаційних ресурсів АТС, коли порушуються встановлені правила розмежування доступу (ПРД) і (або) правові норми з метою реалізації будь-якої з видів загроз для інформації на АТС через канал спеціального неприпустимого регламентом впливу за допомогою штатних засобів доступу на устаткування, програми, дані та процеси (див. розділ 7);

– через канал спеціального неприпустимого регламентом впливу із застосуванням штатних основних або додаткових програмних і (або) технічних засобів станції (але не штатних засобів доступу) на устаткування, програми, дані і процеси, що утворений з метою реалізації будь-якої з видів загроз для інформації на АТС;

– через канал спеціального неприпустимого регламентом впливу на параметри середовища функціонування АТС, що утворений з метою порушень доступності до інформації на АТС;

– через канал спеціального впливу позаштатними програмними і (або) програмно-технічними засобами на елементи устаткування, програми, дані і процеси на АТС, встановленими на передексплуатаційних стадіях і в процесі її експлуатації з метою реалізації будь-якої з видів загроз для інформації на АТС;

– через канал спеціального впливу на компоненти АТС за допомогою закладних пристроїв і (або) програмних закладок, впроваджених у середовище функціонування АТС на передексплуатаційних стадіях і в процесі її експлуатації з метою реалізації будь-яких з видів загроз для інформації на АТС;

– через канал побічних електромагнітних випромінювань і навідів (ПЕМВН) із метою порушень конфіденційності на АТС;

– через канал побічних акусто-електричних перетворень інформативних сигналів на прикінцевому устаткуванні ліній зв'язку з метою порушень конфіденційності інформації на АТС;

– через кількісну і (або) якісну недостатність компонентів і (або) всієї АТС у цілому з метою реалізації будь-якої з видів загроз для інформації на АТС;

– за рахунок використання випадкових збоїв і відмов у роботі устаткування АТС з метою реалізації будь-яких з видів загроз для інформації на АТС;

– за рахунок використання помилок і некоректних (зокрема, зловмисних) дій відповідальних осіб при збереженні критичної інформації на фізичних носіях з метою реалізації будь-яких з видів загроз для інформації на АТС.

9 Моделі порушників

9.1 За порушників на АТС розглядаються суб'єкти , внаслідок навмисних або випадкових дій котрих, і (або) випадкові події, внаслідок настання яких можливі реалізації загроз для інформації.

Розглядаються три групи моделей порушників на АТС. Перша група містить у собі моделі порушників, що реалізують загрози на одній підсистемі АТС (див. розділ 6) з боку іншої підсистеми. Друга група містить у собі моделі порушників, що реалізують загрози на підсистемі керування станцією. Третя група містить у собі моделі порушників, що реалізують загрози на підсистемі КАЗЛ АТС.

Передбачається, що порушник - суб'єкт є кваліфікованим фахівцем, володіє всією технічною інформацією про АТС і, зокрема, про системи і можливі засоби її захисту, а порушник - випадкова подія має найгірший (із позицій власників інформації, що захищається) закон розподілу.

9.2 Кодифікатор моделей порушників на АТС наданий у таблиці 1.

Таблиця 1

Код моделі порушника	Найменування моделі порушника
	Перша група моделей (для порушників, які створюють загрози на одній підсистемі АТС при впливах з боку іншої підсистеми)
МН1.01	Модель порушника ПРД до інформаційних ресурсів підсистеми керування станцією, який діє з боку абонентських ліній
МН1.02	Модель порушника, який використовує помилки або некоректні дії суб'єктів, що допущені на будь-якій із стадій життєвого циклу АТС, з метою реалізації загроз на підсистемі керування шляхом впливу на інформацію з боку підсистеми КАЗЛ
МН1.03	Модель порушника, який використовує програмні і (або) технічні позаштатні пристрої, що встановлені на підсистемі керування АТС, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми КАЗЛ
МН1.04	Модель порушника, який використовує програмно-технічні позаштатні пристрої, що встановлені на підсистемі КАЗЛ АТС, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми керування

Продовження таблиці 1

Код моделі порушника	Найменування моделі порушника
МН1.05	Модель порушника, який використовує якісну недостатність інформаційно-уразливих режимів, функцій і послуг, що надаються АТС, для реалізації загроз на підсистемі КАЗЛ з боку підсистеми керування
	Друга група моделей (для порушників, які створюють загрози на підсистемі керування АТС)
МН2.01	Модель порушника ПРД
МН2.02	Модель порушника, який реалізує неприпустимі впливи через штатні засоби станції (але не штатні засоби доступу) на елементи підсистеми керування АТС
МН2.03	Модель порушника, який реалізує неприпустимі впливи на параметри середовища експлуатації АТС з метою порушень доступності до підсистеми керування
МН2.04	Модель порушника, що впливає позаштатними засобами на елементи підсистеми керування АТС
МН2.05	Модель порушника, який використовує закладні пристрої і (або) програмні закладки, що встановлені на елементах підсистеми керування
МН2.06	Модель порушника через канали ПЕМВН
МН2.07	Модель порушника через канали побічних акусто-електричних перетворень на терміналах обслуговування АТС
МН2.08	Модель порушника, який використовує помилки або некоректні дії суб'єктів доступу до підсистеми керування або її документації, що допущені на передексплуатаційних стадіях життєвого циклу АТС
МН2.09	Модель порушника, який використовує помилки або некоректні дії персоналу АТС при збереженні критичної інформації на фізичних носіях
МН2.10	Модель порушника, який використовує випадкові збої і відмови в роботі підсистеми керування АТС
	Третя група моделей (для порушників, які створюють загрози на підсистемі КАЗЛ АТС)
МН3.01	Модель порушника, який реалізує неприпустимі впливи через штатні засоби станції на елементи підсистеми КАЗЛ АТС
МН3.02	Модель порушника, який реалізує неприпустимі впливи на параметри середовища експлуатації АТС з метою порушень доступності до елементів підсистеми КАЗЛ АТС
МН3.03	Модель порушника, який впливає позаштатними засобами на елементи підсистеми КАЗЛ АТС
МН3.04	Модель порушника, який використовує програмні закладки і (або) апаратні закладні пристрої, що встановлені на підсистемі КАЗЛ АТС
МН3.05	Модель порушника через канали ПЕМВН
МН3.06	Модель порушника через канали побічних акусто-електричних перетворень в абонентських прикінцевих пристроях.

Продовження таблиці 1

Код моделі порушника	Найменування моделі порушника
МН3.07	Модель порушника, який використовує помилки або некоректні дії суб'єктів доступу до підсистеми КАЗЛ або її документації, що допущені на передексплуатаційних стадіях життєвого циклу АТС
МН3.08	Модель порушника, який використовує випадкові збої і відмови в роботі елементів підсистеми КАЗЛ АТС

9.3 Рівні можливостей порушників

9.3.1 Рівні можливостей порушника для моделі МН1.01

Передбачається, що порушник намагається порушити встановлені ПРД до ресурсів підсистеми керування АТС з боку підсистеми КАЗЛ, маючи в розпорядженні штатний абонентський прикінцевий пристрій. Порушник має при цьому єдиний рівень можливостей - можливість вибору прикладної задачі і ведення в її середовищі діалогу, як-от: запуску задач (програм) із фіксованого набору, що реалізують заздалегідь передбачені функції (послуги) щодо опрацювання інформації; діалогу в процесі виконання активних задач; реконфігурації прикінцевого устаткування і наданих послуг засобами прикладного програмного забезпечення.

Для порушника в рамках розглянутої моделі виключається можливість:

- створення і запуску власних програм;

- керування функціонуванням АТС (зокрема, реконфігурацією устаткування) засобами системного програмного забезпечення;

- включення до складу устаткування підсистеми керування АТС позаштатних програмних і (або) технічних засобів.

9.3.2 Рівні можливостей порушників для моделі МН1.02

У рамках моделі МН1.02 розрізняють порушника - джерела помилок або некоректних дій і порушника - реалізатора загроз для інформації на підсистемі керування станцією, що діє з боку підсистеми КАЗЛ.

Передбачається, що порушник -джерело помилок або некоректних дій може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень і може мати можливість доступу до будь-яких штатних механізмів взаємодії авторизованого користувача із середовищем розробки, виготовлення і (або) експлуатації АТС на будь-якій із стадій її життєвого циклу. Порушник - реалізатор загроз також може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень, але діє тільки на стадії промислової експлуатації АТС.

Комбінації можливостей порушників для моделі МН1.02 надані в таблиці 2.

Таблиця 2

Можливості джерела помилок або некоректних дій	Можливості реалізатора загроз для інформації
Помилки або некоректні дії розроблювача (проектувальника) АТС	Можливості абонента АТС
Помилки або некоректні дії розроблювача АТС	Можливості персоналу АТС
Помилки або некоректні дії виготовлювача АТС	Можливості абонента АТС
Помилки або некоректні дії виготовлювача АТС	Можливості персоналу АТС
Помилки або некоректні дії постачальника АТС	Можливості абонента АТС
Помилки або некоректні дії постачальника АТС (у т.ч., у процесі монтажу і введення в експлуатацію АТС)	Можливості персоналу АТС
Помилки або некоректні дії авторизованих користувачів АТС у процесі її експлуатації	Можливості абонента АТС
Помилки або некоректні дії авторизованих користувачів АТС у процесі її експлуатації	Можливості персоналу АТС

9.3.3 Рівні можливостей порушників для моделі МН1.03

У рамках моделі МН1.03 розрізняють порушника - установника технічних і (або) інсталятора програмних позаштатних пристроїв на підсистемі керування АТС і порушника - реалізатора загроз для інформації, який діє з боку підсистеми КАЗЛ.

Передбачається, що порушник - установник (інсталятор) позаштатних пристроїв може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень і може мати можливість доступу до середовища розробки, виготовлення і (або) експлуатації підсистеми керування АТС на будь-якій із стадій її життєвого циклу.

Порушник - реалізатор загроз також може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень, але діє тільки на стадії промислової експлуатації АТС.

Комбінації можливостей порушників для моделі МН1.03 надані в таблиці 3.

Таблиця 3

Можливості установника позаштатних пристроїв	Можливості реалізатора загроз для інформації
Установка апаратних закладних пристроїв і (або) програмних закладок у підсистемі керування на стадії розробки (проектування) АТС	Можливості абонента АТС
Установка апаратних закладних пристроїв і (або) програмних закладок у підсистемі керування на стадії розробки (проектування) АТС	Можливості персоналу АТС

Продовження таблиці 3

Можливості установника позаштатних пристроїв	Можливості реалізатора загроз для інформації
Установка апаратних закладних пристроїв і (або) програмних закладок у підсистемі керування на стадії виготовлення (виробництва)	Можливості абонента АТС
Установка апаратних закладних пристроїв і (або) програмних закладок у підсистемі керування на стадії виготовлення (виробництва) АТС	Можливості персоналу АТС
Установка апаратних закладних пристроїв і (або) програмних закладок у підсистемі керування на стадії поставки (у т.ч., монтажу і введення в експлуатацію)	Можливості абонента АТС
Установка апаратних закладних пристроїв і (або) програмних закладок у підсистемі керування на стадії поставки (у т.ч., монтажу і введення в експлуатацію АТС)	Можливості персоналу АТС
Установка позаштатних апаратних і (або) програмних пристроїв на підсистемі керування АТС у процесі її експлуатації	Можливості абонента АТС
Установка позаштатних апаратних і (або) програмних пристроїв на підсистемі керування АТС у процесі її експлуатації	Можливості персоналу АТС

9.3.4 Рівні можливостей порушників для моделі МН1.04

У рамках моделі МН1.04 розрізняють порушника - установника позаштатних програмно-апаратних пристроїв на підсистемі КАЗЛ і порушника - реалізатора загроз для інформації, який діє з боку підсистеми керування станцією.

Передбачається, що порушник-установник позаштатних пристроїв може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень і може мати можливість доступу до середовища розробки, виготовлення і (або) функціонування підсистеми КАЗЛ АТС на будь-якій із стадій її життєвого циклу.

Порушник - реалізатор загроз також може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень, але діє тільки на стадії промислової експлуатації АТС.

Комбінації можливостей порушників для моделі МН1.04 надані в таблиці 4.

Таблиця 4

Можливості установника позаштатних пристроїв	Можливості реалізатора загроз для інформації
Установка програмно-апаратних закладних пристроїв у підсистемі КАЗЛ на стадії розробки (проектування) АТС	Можливості абонента АТС
Установка програмно-апаратних закладних пристроїв у підсистемі КАЗЛ на стадії розробки (проектування) АТС	Можливості персоналу АТС
Установка програмно-апаратних закладних пристроїв у підсистемі КАЗЛ на стадії виготовлення (виробництва) АТС	Можливості абонента АТС
Установка програмно-апаратних закладних пристроїв у підсистемі КАЗЛ на стадії виготовлення(виробництва) АТС	Можливості персоналу АТС

Продовження таблиці 4

Можливості установника позаштатних пристроїв	Можливості реалізатора загроз для інформації
Установка програмно-апаратних закладних пристроїв у підсистемі КАЗЛ на стадії поставки (у т.ч., монтажу і введення в експлуатацію) АТС	Можливості абонента АТС
Установка програмно-апаратних закладних пристроїв у підсистемі КАЗЛ на стадії поставки (у т.ч., монтажу і введення в експлуатацію) АТС	Можливості персоналу АТС
Установка позаштатних програмно-апаратних пристроїв у підсистемі КАЗЛ АТС на стадії її експлуатації	Можливості абонента АТС
Установка позаштатних програмно-апаратних пристроїв у підсистемі КАЗЛ АТС на стадії її експлуатації	Можливості персоналу АТС

9.3.5 Рівні можливостей порушників для моделі МН1.05

У рамках моделі МН1.05 розрізняють порушника - джерела якісної недостатності режимів, функцій або послуг і порушника - реалізатора загроз на підсистемі КАЗЛ, який діє з боку підсистеми керування станцією.

Можливості порушників передбачаються такими ж, як для моделі МН1.04.

9.3.6 Рівні можливостей порушника для моделі МН2.01

Передбачається, що порушник намагається порушити встановлені ПРД за допомогою використання штатного термінала обслуговування АТС. При цьому рівень можливостей порушника для моделі МН2.01 збігається з рівнем можливостей порушника для моделі МН1.01.

9.3.7 Рівні можливостей порушника для моделі МН2.02

Передбачається, що порушник має повноваження для доступу до програмного забезпечення і (або) до елементів устаткування підсистеми керування АТС.

9.3.8 Рівні можливостей порушника для моделі МН2.03

Передбачається, що порушник намагається викликати збої або відмови в роботі АТС за допомогою виводу параметрів зовнішнього середовища, у якій функціонує система керування станцією, за межі штатних значень (наприклад, шляхом навмисного силового впливу через мережу електроживлення, радіоактивного або теплового опромінення елементів устаткування, порушень у роботі системи енергопостачання або кондиціонування і т.ін.). При цьому враховуються два рівня можливостей порушника: перший - коли порушник знаходиться усередині контрольованої зони і має повноваження для доступу до станційного устаткування АТС; другий - коли порушник перебуває за межами контрольованої зони.

9.3.9 Рівні можливостей порушника для моделі МН2.04

Передбачається, що порушник має повноваження для доступу до програмного забезпечення і (або) до елементів устаткування підсистеми керування АТС.

9.3.10 Рівні можливостей порушника для моделі МН2.05

Передбачається, що порушники (як установник закладних пристроїв, так і реалізатор загроз для інформації) діють на підсистемі керування АТС і мають повноваження для доступу до програмного забезпечення і (або) до елементів устаткування АТС.

9.3.11 Рівні можливостей порушника для моделі МН2.06

Передбачається, що порушник намагається порушити конфіденційність інформації, маючи у своєму розпорядженні сучасні засоби прийому і виділення інформативних параметрів ПЕМВН, що генеруються елементами устаткування підсистеми керування АТС, або навідів на термінальних лініях за рахунок ПЕМВН від зовнішніх джерел. При цьому враховуються два рівня можливостей порушника: перший - коли порушник знаходиться усередині контрольованої зони станційного устаткування АТС; другий - коли порушник перебуває за межами контрольованої зони.

9.3.12 Рівні можливостей порушника для моделі МН2.07

Передбачається, що порушник намагається порушити конфіденційність інформації, маючи у своєму розпорядженні сучасні засоби виділення прийому і посилення інформативних сигналів, що можуть виникати на термінальних лініях зв'язку за рахунок побічних акусто-електричних перетворень інформативних сигналів у термінальному устаткуванні підсистеми керування АТС. При цьому враховується один рівень можливостей порушника - коли порушник має повноваження для доступу до термінальних ліній зв'язку усередині контрольованої зони станційного устаткування АТС.

9.3.13 Рівні можливостей порушників для моделі МН2.08

Передбачається, що порушники (як джерело помилок або некоректних дій, так і реалізатор загроз для інформації) діють на підсистемі керування АТС і мають повноваження для доступу до програмного забезпечення і (або) до елементів устаткування АТС.

9.3.14 Рівні можливостей порушників для моделі МН2.09

Передбачається, що порушники можуть мати повноваження для доступу до критичної інформації на фізичних носіях.

9.3.15 Рівні можливостей порушників для моделі МН2.10

Передбачається два рівня можливостей порушників: перший - можливості абонента АТС; другий - можливості персоналу АТС.

9.3.16 Рівні можливостей порушників для моделі МН3.01

Враховуються два рівня можливостей порушника: перший - коли порушник має повноваження для доступу до елементів устаткування підсистеми КАЗЛ; другий - коли порушник не має повноважень для доступу до елементів устаткування підсистеми КАЗЛ.

Передбачається, що порушник намагається впливати на елементи устаткування підсистеми КАЗЛ, модифікувати виконувані станцією функції або надані абоненту послуги, маючи у своєму розпорядженні сучасні засоби впливу на програмно-апаратні засоби АТС.

9.3.17 Рівні можливостей порушників для моделі МН3.02

Передбачається, що порушник намагається викликати збої або відмови в роботі АТС за допомогою виводу параметрів зовнішнього середовища, у якій функціонує підсистема КАЗЛ, за межі штатних значень. При цьому враховується два рівня можливостей порушника: перший - коли порушник має повноваження для доступу до елементів устаткування підсистеми КАЗЛ; другий - коли порушник такої можливості не має.

9.3.18 Рівні можливостей порушників для моделі МН3.03

Передбачається, що порушник намагається реалізувати загрози для інформації, маючи у своєму розпорядженні сучасні позаштатні засоби впливу, зокрема засоби знімання

інформації з цифрових і аналогових абонентських ліній зв'язку і станційної крос-панелі. При цьому враховуються два рівня можливостей порушника: перший - коли порушник має повноваження для доступу до елементів підсистеми КАЗЛ; другий - коли порушник таких повноважень не має.

9.3.19 Рівні можливостей порушників для моделі МН3.04

Передбачається, що порушники (як установник закладних пристроїв, так і реалізатор загроз для інформації) діють на підсистемі КАЗЛ і їхні рівні можливостей збігаються з рівнями можливостей для моделі МН2.05.

9.3.20 Рівні можливостей порушників для моделі МН3.05

Передбачається, що порушник намагається порушити конфіденційність інформації, маючи у своєму розпорядженні сучасні засоби прийому і виділення інформативних параметрів ПЕМВН, що генеруються елементами устаткування абонентських ліній зв'язку, або навідів у лінії зв'язку за рахунок ПЕМВН від зовнішніх джерел інформації. При цьому враховуються два рівня можливостей порушника: перший - коли порушник знаходиться усередині контрольованих зон підсистеми КАЗЛ; другий - коли порушник перебуває за межами контрольованих зон.

9.3.21 Рівні можливостей порушників для моделі МН3.06

Передбачається, що порушник намагається порушити конфіденційність інформації, маючи у своєму розпорядженні сучасні засоби виділення, прийому і посилення інформативних сигналів, що можуть виникати на абонентських лініях зв'язку за рахунок побічних акусто-електричних перетворень в абонентських прикінцевих пристроях. При цьому враховуються два рівня можливостей порушника: перший - коли порушник має повноваження для доступу до абонентських ліній зв'язку; другий - коли порушник не має повноважень для доступу до абонентських ліній зв'язку.

9.3.22 Рівні можливостей порушників для моделі МН3.07

Передбачається, що порушники (як джерело помилок або некоректних дій, так і реалізатор загроз для інформації) діють на підсистемі КАЗЛ і їхні рівні можливостей збігаються з рівнями можливостей порушників для моделі МН1.02.

9.3.23 Рівні можливостей порушників для моделі МН3.08.

Передбачається два рівня можливостей порушника: перший - можливості абонента АТС; другий - можливості персоналу АТС.

9.4 Основні способи реалізації загроз для інформації

9.4.1 До основних способів порушень у рамках моделі МН1.01 відносяться:

- безпосереднє звертання до об'єктів доступу шляхом ушкодження системи ідентифікації й автентифікації користувачів (наприклад, шляхом добору вірного пароля і т.ін.);

- маніпуляція штатними засобами доступу підсистеми КАЗЛ, що дозволяє внаслідок кількісної і (або) якісної недостатності компонентів АТС (або недосконалості архітектури або конструкції АТС у цілому) здійснити доступ до об'єктів підсистеми керування станцією (зокрема, шляхом створення каналів доступу до інформаційних ресурсів в обхід засобів і механізмів захисту);

- модифікація засобів захисту на підсистемі КАЗЛ, що дозволяє здійснити НСД до об'єктів на підсистемі керування.

9.4.2 До основного способу порушень у рамках моделі МН1.02 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі КАЗЛ АТС, що дозволяє внаслідок помилок або некоректних дій суб'єктів доступу до середовищ проектування, виготовлення або експлуатації АТС реалізувати загрози для інформації.

9.4.3 До основного способу порушень у рамках моделі МН1.03 відноситься установка позаштатних апаратних і (або) інсталяція позаштатних програмних засобів у підсистемі керування на передексплуатаційних стадіях життєвого циклу АТС з наступною їхньою активізацією через спеціальні канали впливу з боку підсистеми КАЗЛ на стадії промислової експлуатації станції з метою реалізації будь-якої з видів загроз (див. розділ 7).

9.4.4 До основного способу порушень у рамках моделі МН1.04 відноситься установка програмно-апаратних позаштатних пристроїв на підсистемі КАЗЛ АТС на будь-якій із стадій життєвого циклу АТС з наступною їхньою активізацією через спеціальні канали впливу з боку підсистеми керування на стадії промислової експлуатації станції з метою реалізації будь-якої з видів загроз.

9.4.5 До основного способу порушень у рамках моделі МН1.05 відноситься використання "слабких місць" в захисті або модифікація з боку підсистеми керування порядку (або умов) роботи інформаційно-уразливих режимів, функцій і послуг, що надаються АТС, з метою реалізації загроз на підсистемі КАЗЛ станції.

9.4.6 До основних способів порушень у рамках моделі МН2.01 відносяться:

- безпосереднє звертання до об'єктів доступу шляхом ушкодження системи ідентифікації й автентифікації користувачів (наприклад, шляхом добору вірного пароля і т.ін.);

- штатна маніпуляція штатними засобами підсистеми керування, що дозволяє внаслідок кількісної і (або) якісної недостатності компонентів АТС (або недосконалості архітектури або конструкції АТС у цілому) здійснити доступ до об'єктів підсистеми керування станцією;

- позаштатна маніпуляція штатними засобами підсистеми керування, що дозволяє здійснити доступ до об'єктів на підсистемі керування (зокрема, шляхом створення каналів доступу до інформаційних ресурсів, що захищаються, в обхід засобів захисту);

- модифікація засобів захисту на підсистемі керування станцією, що дозволяє здійснити НСД до об'єктів на підсистемі керування.

9.4.7 До основного способу порушень у рамках моделі МН2.02 відноситься неприпустимий вплив через штатні засоби АТС (але не штатні засоби доступу – системні термінали, віддалені засоби доступу через модеми і т.ін.) на елементи системи керування станцією з метою реалізації будь - якої із загроз (див. розділ 7).

9.4.8 До основного способу порушень у рамках моделі МН2.03 відноситься маніпуляція засобами впливу на параметри середовища експлуатації АТС з метою організації навмисних збоїв і відмов у роботі АТС шляхом виводу параметрів устаткування підсистеми керування станцією за межі штатних значень.

9.4.9 До основного способу порушень у рамках моделі МН2.04 відноситься вплив позаштатними технічними або програмно-технічними засобами на елементи підсистеми керування АТС з метою реалізації будь-якої з видів загроз (див. розділ 7).

9.4.10 До основного способу порушень у рамках моделі МН2.05 відноситься установка апаратних закладних пристроїв і (або) інсталяція програмних закладок на підсистемі керування на будь-якій із стадій життєвого циклу АТС з наступною їхньою активізацією на стадії промислової експлуатації станції з метою реалізації будь-якої із основних видів загроз на АТС.

9.4.11 До основного способу порушень у рамках моделі МН2.06 відноситься прийом і виділення інформативних параметрів ПЕМВН від елементів підсистеми керування станцією (зокрема, від терміналів обслуговування, периферійних пристроїв і т.ін.).

9.4.12 До основних способів порушень у рамках моделі МН2.07 відносяться:

- зняття інформативних сигналів із комунікаційних ліній, що утворюються на виході терміналів обслуговування АТС внаслідок побічних акусто-електричних перетворень;

- модуляція штучно створюваного несучого коливання інформативними сигналами в лінії ("ВЧ -накачка") з метою полегшення процесу транспортування знятих сигналів за межі контрольованої зони.

9.4.13 До основного способу порушень у рамках моделі МН2.08 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі керування станцією, що дозволяє внаслідок помилок або некоректних дій суб'єктів доступу реалізувати будь-яку із основних видів загроз на АТС.

9.4.14 До основних способів порушень у рамках моделі МН2.09 відносяться:

- несанкціоноване ознайомлення із критичною інформацією, що зберігається на фізичних носіях, з метою реалізації будь-якої із загроз (див. розділ 7);

- порушення цілісності критичної інформації.

9.4.15 До основного способу порушень у рамках моделі МН2.10 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі керування АТС, що дозволяє використовувати випадкові збої і відмови в роботі АТС з метою реалізації будь-якої із основних видів загроз.

9.4.16 До основного способу порушень у рамках моделі МН3.01 відноситься позаштатний вплив штатними технічними або програмно-технічними засобами на елементи підсистеми КАЗЛ АТС з метою реалізації будь-якої із видів загроз (див. розділ 7).

9.4.17 До основного способу порушень у рамках моделі МН3.02 відноситься маніпуляція засобами впливу на параметри середовища експлуатації АТС з метою організації навмисних збоїв і відмов у роботі АТС шляхом виводу параметрів устаткування підсистеми КАЗЛ АТС за межі штатних значень.

9.4.18 До основного способу порушень у рамках моделі МН3.03 відноситься безпосереднє під'єднання (гальванічне, індуктивне, ємнісне і т.ін.) апаратури прослуховування до абонентської лінії або крос-панелі з наступним записом знятої інформації на фізичні носії і (або) її передачею за межі контрольованої зони через схований канал передачі.

9.4.19 До основного способу порушень у рамках моделі МН3.04 відноситься установка програмних закладок і (або) апаратних закладних пристроїв на підсистемі КАЗЛ на будь-якій із стадій життєвого циклу АТС з наступною їхньою активізацією через канали спеціального впливу на стадії промислової експлуатації станції з метою реалізації будь-якої із видів загроз на АТС.

9.4.20 До основних способів порушень у рамках моделі МН3.05 відносяться:

- прийом і виділення інформативних параметрів побічних електромагнітних випромінювань від елементів підсистеми КАЗЛ (в основному, від цифрових абонентських ліній) як усередині, так і поза межами контрольованих зон;

- прийом і виділення інформативних параметрів побічних електромагнітних навідів від елементів підсистеми КАЗЛ (зокрема, від цифрових абонентських ліній) у ланцюгах електроживлення, пожежної й охоронної сигналізації і т. ін.;

- зняття інформативних сигналів - електромагнітних навідів від джерел інформативних випромінювань, що знаходяться в зонах прикінцевих абонентських пристроїв, на абонентських лініях зв'язку АТС.

9.4.21 До основних способів порушень у рамках моделі МН3.06 відносяться:

- зняття інформативних сигналів з аналогових абонентських ліній, що утворюються на виході прикінцевих пристроїв в результаті побічних акусто-електричних перетворень у режимі чекання телефонного виклику(у режимі "покладеної трубки");

- модуляція штучно створюваного несучого коливання інформативними сигналами в аналоговій абонентської лінії ("ВЧ-накачка") з метою полегшення процесу транспортування знятих сигналів за межі контрольованої зони;

- демодуляція інформативної обгинаючої сигналів лінійного коду в цифрових абонентських лініях, утвореної через побічні акусто-електричні перетворення в цифрових прикінцевих пристроях, із наступним записом знятої інформації на фізичні носії і (або) її передачею за межі контрольованої зони через схований канал передачі.

9.4.22 До основного способу порушень у рамках моделі МН3.07 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і технічними засобами на підсистемі КАЗЛ, що дозволяє внаслідок помилок або некоректних дій суб'єктів доступу реалізувати будь-яку із видів загроз.

9.4.23 До основного способу порушень у рамках моделі МН3.08 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі КАЗЛ АТС, що дозволяє використовувати випадкові збої і відмови в роботі АТС з метою реалізації будь-якої із видів загроз.

10 Види забезпечення систем ТЗІ на АТС

10.1 Забезпечення систем ТЗІ на АТС здійснюється:

- сукупністю технічних і (або) програмних підсистем захисту, що функціонують на стадії її промислової експлуатації;

- системою організаційно-технічних заходів;

- системою ліквідації наслідків реалізованих загроз для інформації на АТС;

- системою керування засобами ТЗІ.

10.2 Підсистеми захисту на АТС класифікуються за способами здійснення загроз і в сукупності повинні забезпечувати реалізацію на практиці обраної моделі захисту.

10.3 Система організаційно-технічних заходів, що здійснюється на всіх стадіях життєвого циклу АТС, повинна знизити рівні кількісної і якісної недостатності компонентів і всієї АТС у цілому до можливих і (або) припустимих значень.

10.4 Система ліквідації наслідків реалізованих загроз для інформації, що являє собою сукупність програмно-апаратних засобів і відповідних організаційних заходів, повинна знизити рівень втрат від реалізованих загроз для інформації до можливих і (або) припустимих меж.

10.5 Система керування засобами ТЗІ повинна забезпечувати безперервний контроль і підтримку певного рівня захищеності інформації на АТС на стадії її промислової експлуатації.

10.6 Шляхи реалізації систем ТЗІ залежать від конкретних особливостей застосування АТС, а ресурси, що пов'язані з ТЗІ, включаються в об'єкти доступу і, отже, потребують

захисту.

11 Функції систем захисту

Системи ТЗІ на АТС виконують функції, що забезпечують реалізацію визначеної номенклатури функціональних послуг захисту згідно з ISO 7498-2 (Рекомендацією X.800 CCITT) та НД ТЗІ 2.5-001-99.

11.1 Основними функціями підсистем захисту від несанкціонованих впливів через штатні засоби доступу є:

- реалізація ПРД суб'єктів і їхніх процесів із боку моніторів обслуговування до програм, даних, процесів і пристроїв на підсистемі керування АТС;

- реалізація ПРД суб'єктів і їхніх процесів із боку телефонних комутаторів і прикінцевих абонентських пристроїв до сервісних функцій і послуг АТС;

- контроль доступу до підсистеми керування станцією з боку віддалених терміналів обслуговування;

- ізоляція програм, що виконуються в інтересах суб'єкта, від інших суб'єктів;

- керування потоками даних і команд з метою запобігання помилкових з'єднань, помилкового надання послуг і відмов в обслуговуванні ;

- ідентифікація й упізнання (автентифікація) суб'єктів;

- реєстрація дій суб'єкта і його процесу;

- надання можливостей вилучення або включення нових суб'єктів і об'єктів доступу , а також зміни повноважень суб'єктів;

- реакція на спроби НСД, наприклад, сигналізація, блокування, знищення ресурсу, відновлення після НСД;

- шифрація інформаційних ресурсів;

- тестування засобів захисту від НСД;

- очищення робочих областей пам'яті ЕОМ після завершення роботи з даними, що захищаються;

- облік вихідних друкарських і графічних форм і твердих копій;

- контроль цілісності програмної й інформаційної частин системи розмежування доступу (СРД).

11.2 Основними функціями підсистем захисту від позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби АТС є:

- виявлення позаштатних впливів на елементи устаткування, програми, дані і процеси;

- реєстрація позаштатних впливів;

- реакція на спроби позаштатних впливів, наприклад, сигналізація, блокування, знищення ресурсу, відновлення після позаштатних впливів;

- моніторинг з метою виявлення позаштатних впливів;

- ідентифікація і розпізнавання процесів;

- реалізація ПРД до інформаційних ресурсів не тільки для процесів, що ініціюються з боку терміналів обслуговування, телефонних комутаторів і прикінцевих абонентських пристроїв, але і для процесів, що ініціюються з боку потенційно небезпечних місць

позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби АТС;

- контроль цілісності програмної й інформаційної частин засобів захисту від позаштатних впливів;

- тестування засобів захисту від позаштатних впливів.

11.3 Основними функціями підсистем захисту від позаштатних впливів на параметри середовища експлуатації АТС є:

- виявлення позаштатних впливів на параметри середовища експлуатації АТС;

- реєстрація таких позаштатних впливів;

- реакція на спроби таких позаштатних впливів, наприклад, сигналізація, блокування, відновлення після позаштатних впливів;

- моніторинг з метою виявлення позаштатних впливів;

- введення в дію засобів протидії непередбаченим змінам параметрів середовища експлуатації АТС;

- керування засобами нейтралізації позаштатних впливів на параметри середовища експлуатації АТС (вмикання /вимикання і т.ін.);

- контроль цілісності апаратної, програмної й інформаційної частин засобів захисту від позаштатних впливів;

- тестування засобів захисту від позаштатних впливів.

11.4 Основними функціями підсистем захисту від впливів з використанням позаштатних технічних і (або) програмно-технічних засобів на елементи устаткування в процесі експлуатації АТС є:

- виявлення впливів позаштатними засобами на елементи устаткування;

- реєстрація таких позаштатних впливів;

- реакція на спроби таких позаштатних впливів, наприклад, сигналізація, блокування, нейтралізація спроб реалізації загроз, знешкодження (вивід із працездатного стана) атакуючої апаратури, відновлення після позаштатних впливів;

- керування засобами нейтралізації позаштатних впливів на елементи устаткування АТС (умикання/вимикання і т.ін.);

- контроль цілісності апаратної, програмної й інформаційної частин засобів системи захисту;

- тестування засобів системи захисту.

11.5 Основними функціями підсистем захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, що встановлені в процесі її експлуатації, є:

- виявлення впливів позаштатними засобами на програми, дані і процеси на АТС;

- реєстрація таких позаштатних впливів;

- реакція на спроби таких позаштатних впливів, наприклад, сигналізація, блокування, відновлення після позаштатних впливів;

- моніторинг з метою виявлення позаштатних впливів;

- ідентифікація і розпізнавання процесів;

- реалізація ПРД до інформаційних ресурсів АТС для процесів, що ініціюються

позаштатними програмними і (або) програмно-технічними засобами;

- контроль цілісності апаратної, програмної й інформаційної частин засобів підсистеми захисту;

- тестування засобів підсистеми захисту.

11.6 Основними функціями підсистем захисту від впливів закладних пристроїв і програмних закладок є:

- виявлення закладних пристроїв і програмних закладок;

- реєстрація впливів закладних пристроїв і програмних закладок;

- нейтралізація (знешкодження) закладних пристроїв і програмних закладок;

- реакція на впливи закладних пристроїв і програмних закладок, наприклад, сигналізація, блокування, нейтралізація спроб реалізації загроз, відновлення після впливів;

- контроль цілісності засобів підсистеми захисту;

- тестування засобів підсистеми захисту.

11.7 Основними функціями технічних або програмно-технічних підсистем захисту від витоків інформації через канали ПЕМВН є:

- виявлення ПЕМВН від елементів АТС (головним чином, випромінювань від абонентських ліній і терміналів обслуговування);

- виявлення електромагнітних навідів в елементах АТС (головним чином, в абонентських лініях) від джерел інформативних випромінювань у зонах розміщення елементів АТС;

- придушення (ослаблення, екранування) ПЕМВН від елементів АТС;

- придушення електромагнітних навідів в елементах АТС від джерел інформативних випромінювань у зонах розміщення елементів АТС;

- нейтралізація інформативних складових ПЕМВН (наприклад, маскуючим шумоподібним сигналом) від елементів АТС;

- нейтралізація електромагнітних навідів в елементах АТС від джерел інформативних випромінювань у зонах розміщення елементів АТС;

- моніторинг з метою виявлення перевищень припустимих значень ПЕМВН;

- тестування засобів підсистеми захисту від витоку через канали ПЕМВН.

11.8 Основними функціями технічних засобів захисту від витоків інформації через канали побічних акусто-електричних перетворень є:

- виявлення інформативних сигналів - продуктів побічних акусто-електричних перетворень на виході прикінцевих пристроїв аналогових абонентських ліній в режимі чекання виклику;

- виявлення інформативних сигналів акусто-електричних перетворень у цифрових абонентських лініях (як цифрових, так і аналогових складових);

- виявлення інформативних сигналів - продуктів побічних акусто-електричних перетворень на виході термінальних пристроїв підсистеми керування станцією;

- виявлення сторонніх високочастотних коливань (так званих сигналів "ВЧ-накачки") в абонентських і термінальних лініях зв'язку;

- виявлення випромінювань при "ВЧ-накачці" від абонентських ліній;

- придушення (ослаблення) сигналів акусто-електричних перетворень в аналогових абонентських лініях;

- придушення сигналів акусто-електричних перетворень у цифрових абонентських лініях(як цифрових, так і аналогових складових);

- придушення сигналів акусто-електричних перетворень у термінальних лініях зв'язку підсистеми керування станцією;

- придушення сигналів " ВЧ-накачки" і випромінювань при "ВЧ-накачці" від абонентських ліній;

- нейтралізація інформативних сигналів акусто-електричних перетворень в аналогових абонентських лініях у режимі чекання виклику;

- нейтралізація інформативних сигналів акусто-електричних перетворень у цифрових абонентських лініях (як цифрових, так і аналогових складових);

- нейтралізація інформативних сигналів акусто-електричних перетворень у термінальних лініях підсистеми керування станцією ;

- моніторинг з метою виявлення сигналів "ВЧ-накачки" в абонентських лініях зв'язку;

- моніторинг з метою виявлення випромінювань при "ВЧ - накачці" від абонентських ліній зв'язку;

- тестування засобів підсистеми захисту від витоку через канали побічних акусто-електричних перетворень.

11.9 Основними функціями підсистем захисту від якісної недостатності інформаційно уразливих режимів, функцій і послуг, що надаються АТС, є:

- ідентифікація і виявлення моментів активізації інформаційно уразливих режимів, функцій і послуг;

- сигналізація (оповіщення суб'єктів) про активний стан інформаційно уразливих режимів, функцій і послуг;

- придушення каналів витоку інформації в інформаційно уразливих режимах, функціях і послугах;

- контроль цілісності програмної й інформаційної частин засобів підсистеми захисту від якісної недостатності;

- тестування засобів підсистеми захисту від якісної недостатності.

11.10 Основними функціями підсистем захисту від збоїв і відмов у роботі АТС є:

- виявлення збоїв і відмов;

- реєстрація збоїв і відмов;

- аварійне завершення активних процесів;

- керування надлишковими ресурсами з метою протидії збоям і відмовам у роботі АТС;

- контроль цілісності програмної й інформаційної частин засобів підсистеми захисту від збоїв і відмов;

- тестування засобів підсистеми захисту від збоїв і відмов.

11.11 Основними функціями програмних і (або) технічних підсистем захисту від загроз у системах збереження інформації на фізичних носіях є:

- виявлення спроб несанкціонованого впливу на інформацію;

- реєстрація спроб впливу на інформацію;

- реакція на спроби несанкціонованих впливів, наприклад, сигналізація, відмова в доступі, знищення інформації, відновлення після впливів;

- ідентифікація й автентифікація суб'єктів доступу;

- реалізація ПРД до інформаційних ресурсів на фізичних носіях;

- шифрація інформаційних ресурсів;

- контроль цілісності програмної й інформаційної частин засобів підсистеми захисту;

- тестування засобів підсистеми захисту.

11.12 Основними функціями систем ліквідації наслідків реалізованих загроз для інформації на АТС є:

- виявлення фактів реалізації загроз;

- реєстрація фактів реалізації загроз;

- реакція на факти реалізації загроз, наприклад, індикація, оповіщення, локалізація і (або) нейтралізація наслідків;

- відновлення після реалізації загроз;

- контроль цілісності програмної й інформаційної частин системи ліквідації наслідків реалізованих загроз;

- класифікація реалізованих загроз і їхнього статистичного опрацювання за певні періоди функціонування АТС;

- тестування засобів системи ліквідації наслідків реалізованих загроз.

11.13 Основними функціями систем керування засобами ТЗІ є:

- досягнення відповідності прийнятих (затверджених) моделей порушників до реальних загроз для інформаційних ресурсів, які можуть мати місце у конкретних поточних умовах застосування АТС;

- досягнення адекватності прийнятої (затвердженої) моделі захисту прийнятим (затвердженим) моделям порушників;

- керування засобами ТЗІ в реальному масштабі часу з метою підтримки певного рівня захищеності інформаційних ресурсів АТС;

- виявлення моментів появи дестабілізуючих чинників, спроб реалізації загроз для інформаційних ресурсів АТС;

- реакція на появу дестабілізуючих чинників і спроби реалізації загроз (наприклад, оповіщення, реєстрація, вмикання засобів захисту т.і.);

- тестування інформаційних ресурсів і засобів ТЗІ, включаючи засоби керування системою ТЗІ;

- моніторинг інформаційних ресурсів і засобів ТЗІ;

- контроль цілісності засобів ТЗІ, включаючи засоби керування системою ТЗІ.

12 Функціональні послуги захисту на АТС

12.1 Функціональна послуга захисту (ФПЗ) являє собою взаємопов'язаний набір виконуваних у середовищі експлуатації АТС елементарних функцій, що дозволяє протистояти певній множині загроз для інформації.

У найпростішому випадку ФПЗ є одна елементарна функція, спрямована на протидію визначеній одній загрозі.

З позицій ТЗІ АТС разом із реалізованою на ній системою захисту розглядається як набір ФПЗ.

Нормовані специфікації ФПЗ, структуровані за видами загроз для інформації і за способами здійснення цих загроз, наведені в НД ТЗІ 2.5-001-99 .

12.2 У ТЗ та ТУ на АТС повинні бути наведені вимоги до ФПЗ згідно з НД ТЗІ 2.5-001-99.

13 Засоби і механізми захисту на АТС

13.1 ФПЗ на АТС здійснюються за допомогою конкретних засобів і механізмів. Засоби і механізми захисту необхідно розглядати в двох аспектах - із позицій їхньої ефективності і коректності. При цьому під ефективністю засобу або механізму захисту розуміється його спроможність протистояти як прямим атакам, так і всіляким лазівкам, що пов'язані з роботою засобу або механізму захисту в конкретних умовах застосування (зокрема, спроможність протистояти відключенням, обходам, ушкодженням, обманам, провокуванням і т.ін.). Під коректністю засобу або механізму захисту розуміється його спроможність правильно реалізувати визначену ФПЗ.

13.2 Спроможність механізму захисту протистояти прямим атакам (тобто, спробам його безпосереднього злому) називається стійкістю (потужністю) механізму. З метою оцінки захищеності АТС специфікуються три рівня стійкості механізмів захисту (базовий, середній і високий). Нормовані специфікації рівнів стійкості механізмів захисту наведені в НД ТЗІ 2.5 - 001 - 99 .

14 Порядок виконання робіт з ТЗІ на АТС

14.1 Порядок виконання робіт з ТЗІ на АТС регламентується ДСТУ 3396.1-96 і НД ТЗІ 2.7-001-99.

15 Оцінка ефективності захисту

15.1 Для одержання впевненості в тому, що інформаційні ресурси АТС захищені з очікуваною якістю від витоку, спеціальних впливів і НСД, необхідно підтвердження досягнутого рівня ефективності такого захисту з боку незалежного оцінювача.

15.2 Згідно з критеріями ITSEC та НД ТЗІ 2.3 - 001 - 99 оцінка захищеності інформації на АТС робиться у двох напрямках.

Перший напрямок містить у собі оцінку коректності (тобто, слушності) створеної на АТС системи ТЗІ, включаючи оцінку коректності моделі захисту, реалізованого комплексу засобів і механізмів захисту, результатів аналізу на відсутність "слабких місць" у захисті.

Другий напрямок містить у собі оцінку рівня довіри до коректності реалізованої на АТС системи ТЗІ. Така оцінка виконується на базі різної повноти і глибини знань про середовище створення та експлуатації АТС, а також про систему ТЗІ до неї.

15.3 Умови, вимоги і показники, згідно яких оцінюється коректність системи ТЗІ, називаються критеріями дієвості. Це основні функціональні критерії, що дозволяють оцінити ефективність захисту.

Критерії дієвості надані в НД ТЗІ 3.7-002-99 і грунтуються на специфікаціях ФПЗ, які, у свою чергу, викладені в НД ТЗІ 2.5-001-99 .

15.4. Рівень довіри до коректності системи ТЗІ специфікується за сьома можливими

градаціями: Е0, Е1, Е2, Е3, Е4, Е5 і Е6. Найнижчий рівень довірчої оцінки - Е0 означає недостатню довіру до коректності системи ТЗІ на оцінюваній АТС. Рівень довіри Е1 є початковим рівнем, нижче якого раціональна довіра не зберігається. Рівень Е6 специфікує вищий ступінь довіри. Інші рівні є проміжними.

У НД ТЗІ 2.5-003-99 надані специфікації довірчих оцінок коректності (тобто, нормовані вимоги і умови) для всіх шести градацій рівнів довіри (крім рівня Е0) до коректності системи ТЗІ, що створена на АТС.

Деякі специфікації довірчих оцінок базуються на специфікаціях гарантій захисту, які, у свою чергу, викадені в НД ТЗІ 2.5-002-99 .