УДК 004.056.5

# ПРИНЦИПИ ТА ПОРЯДОК РОЗРОБКИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

*Ю.В. ЗЕМЛЯНКО, О.А. ЗАМУЛА, О.О. ТКАЧ, Н.І. ЛИТВИНОВА, Я.А. ПЕРЕСІЧАНСЬКА*

Розглядається порядок здійснення заходів та засобів при створенні комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах.

*Ключові слова:* комплексні системи захисту інформації, інформаційно-телекомунікаційні системи.

## ВСТУП

Забезпечення безпеки інформації у інформаційно-телекомунікаційних системах здійснюється шляхом створення та впровадження комплексних систем захисту інформації.

Комплексна система захисту інформації (рис. 1) – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від несанкціонованого доступу.

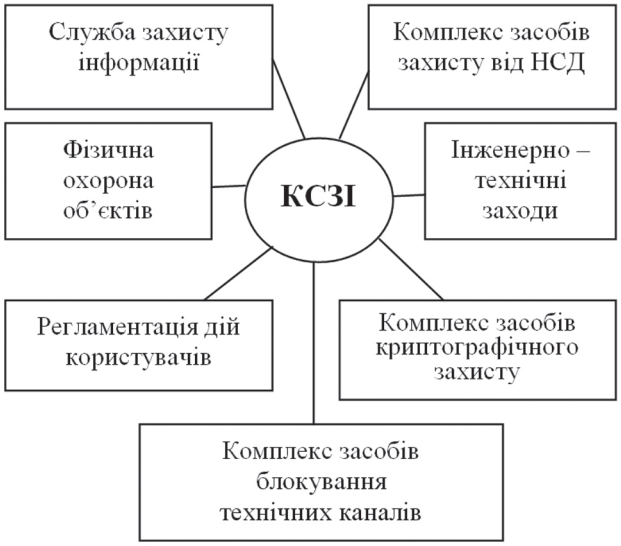


Рис. 1. Комплексна система захисту інформації

## 1. ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

В Законі України «Про захист інформації в інформаційно-телекомунікаційних системах визначено: «Інформація, яка є власністю держави або інформація з обмеженим доступом, вимога щодо якості якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (далі – КСЗІ) з підтвердженою відповідністю». В зазначеному Законі КСЗІ розглядається як взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [1].

Захист інформації є складовою частиною робіт зі створення та експлуатації інформаційно-телекомунікаційних систем (далі – ІТС) і повинен здійснюватися на всіх етапах життєвого циклу ІТС. У ряді чинних нормативно-правових документах визначається, що захист інформації в ІТС забезпечується:

– впровадженням комплексної системи захисту інформації;

– дотриманням суб'єктами відносин, пов'язаних з обробкою інформації в ІТС, законодавства України та нормативних документів у сфері захисту інформації;

– використанням засобів електронно-обчислювальної техніки, програмного забезпечення, телекомунікаційного обладнання, а також засобів захисту інформації, які відповідають вимогам законодавства України щодо захисту інформації.

## 2. ПОРЯДОК СТВОРЕННЯ КСЗІ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Роботи зі створення КСЗІ виконуються організацією-власником ІТС. За умови відсутності у неї відповідних ліцензій або дозволу на здійснення окремих видів робіт із захисту інформації до виконання цих робіт залучаються суб'єкти господарювання, які мають такі ліцензії. Дозвіл на проведення робіт з технічного захисту інформації (далі – ТЗІ) для власних потреб дається Державною службою спеціального зв'язку та захисту інформації (далі – ДССЗЗІ) України у порядку, який визначено Положенням про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. [2]

КСЗІ розробляється і впроваджується в ІТС, що створюються, а також у діючих ІТС, якщо виникла необхідність забезпечення в них захисту інформації.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розробку і впровадження інформаційної технології, що забезпечує обробку інформації в ІТС згідно з вимогами, встановленими державними стандартами, нормативно-правовими актами та нормативними документами у сфері захисту інформації.

Комплексна система захисту інформації є невід'ємною складовою частиною автоматизованої системи (далі – АС) і на неї поширюються всі вимоги державних стандартів щодо створення АС.

Для створення КСЗІ використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок

за результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

**2.1. Послідовність робіт зі створення КСЗІ**

Нормативними документами в сфері ТЗІ визначений порядок проведення робіт зі створення КСЗІ. Основними етапами створення КСЗІ є:

– формування служби захисту інформації (призначення відповідальної особи) для організації робіт зі створення КСЗІ, її експлуатації та контролю за станом захищеності інформації;

– обстеження умов функціонування ІТС та розробка технічного завдання на створення КСЗІ;

– розробка та реалізація проекту КСЗІ;

– введення КСЗІ в дію та оцінка захищеності інформаційних ресурсів ІТС. [2]

Стадії та етапи робіт, які виконуються під час створення КСЗІ в конкретній ІТС, їх зміст і результати, терміни виконання визначаються технічним завданням на створення КСЗІ та договорами між замовником і виконавцями робіт.

Вимоги щодо захисту інформації, які реалізуються КСЗІ, визначаються необхідним рівнем забезпечення властивостей, що характеризують захищеність інформації: цілісність, конфіденційність, доступність.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

– витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

– несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін.;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються рівнем критичності оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС відповідно до нормативних документів з захисту інформації.

Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, яка становить державну таємницю або коли необхідність цього визначена власником інформації.

Створення комплексу засобів захисту(далі – КЗЗ) інформації від несанкціонованого доступу (далі – НСД) здійснюється у всіх ІТС, де обробляється інформація, яка є власністю держави або що відноситься до державної таємниці, або до окремих видів інформації, захист яких гарантується державою, а також в ІТС, де така необхідність визначена власником інформації.

Порядок розробки, впровадження, використання у складі КСЗІ засобів і систем криптографічного захисту інформації регламентується нормативно-правовими актами та нормативними документами з криптографічного захисту інформації.

**2.2. Етапи створення КСЗІ**

**1 етап.** Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ

На цьому етапі в загальному випадку виконується:

– аналіз нормативно-правових актів, на підставі яких можуть встановлюватися обмеження доступу до певних видів інформації або заборона такого обмеження, визначається необхідність забезпечення захисту інформації згідно з іншими критеріями;

– визначаються переліки інформації, що підлягає автоматизованій обробці, і здійснюється її класифікація щодо рівня обмеження доступу до неї, вимог щодо забезпечення цілісності та вимог щодо забезпечення доступності відповідно до нормативно-правових актів.

При обстеженні ІТС розглядається як організаційно – технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС).

Метою обстеження є опис кожного середовища функціонування ІТС та виявлення в них елементів, які безпосередньо або опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

**2 етап.** Формування політики безпеки

На цьому етапі здійснюється:

– аналіз ризиків (вивчення моделі загроз та моделі порушника, можливих наслідків від реалізації потенційних загроз);

– визначення вимог до заходів, методів і засобів захисту інформації;

– вибір основних рішень з протидії всім суттєвим загрозам, формування вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, а також регламентують діяльність користувачів всіх категорій;

– документальне оформлення політики безпеки інформації.

Політика безпеки повинна враховувати особливості окремих компонентів КСЗІ та може розроблятися для ІТС в цілому, для окремих складових компонента, для окремої функціональної задачі, для окремої технології обробки інформа-

ції. Політика безпеки оформляється у вигляді окремого документа Плану захисту.

**3 етап.** Розробка технічного завдання (далі – ТЗ) на створення КСЗІ

Технічне завдання на створення КСЗІ в ІТС є вихідним організаційно-технічним документом, в якому визначаються вимоги щодо захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

Технічне завдання на створення КСЗІ розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу ІТС.

ТЗ на КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

ТЗ на КСЗІ може бути оформлений:

– у вигляді окремого розділу загальної технічної задачі на створення ІТС;

– у вигляді окремого (часткового) ТЗ;

– у вигляді доповнення до загального ТЗ на створення ІТС.

Для інтегрованих ІТС (що складаються з декількох окремих інформаційних чи телекомунікаційних систем, які можуть функціонувати як самостійно, так і взаємодіяти між собою) рекомендується для кожної із складових частин ІТС створювати окремі КСЗІ і оформляти вимоги окремими ТЗ. Можлива розробка одного ТЗ на кілька однотипних складових частин ІТС, вказавши існуючі між ними відмінності або особливості. [6]

**4 етап.** Розробка і реалізація проекту КСЗІ в ІТС

Проект КСЗІ розробляється на підставі та у відповідності з Технічним завданням на створення ІТС і виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робоча документація.

При розробці проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і засобів захисту інформації.

Виконується розробка спільних рішень, необхідних для реалізації вимог ТЗ на КСЗІ, щодо організаційної структури КСЗІ, структури технічних і програмних засобів, алгоритмів функціонування та умов використання засобів захисту, реалізації визначених функціональним профілем захищеності послуг безпеки інформації.

**5 етап.** Введення КСЗІ в дію

На цьому етапі повинна бути завершена розробка КСЗІ і затверджені документи, які входять до Плану захисту.

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів) основним положенням та процедурами документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації.

Проводиться атестація впровадженого комплексу технічного захисту інформації від витоку технічними каналами, за результатами якого видається документ: «Акт атестації комплексу технічного захисту інформації».

Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності комплексу засобів захисту інформації від НСД.

Під час інсталяції повинні бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, механізми контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об'єктах ІТС, їх створення, модифікації, архівування, знищення, експорту / імпорту із системи.

**6 етап.** Попередні випробування

Метою попередніх випробувань є перевірка працездатності КСЗІ, її відповідності технічним завданням і визначення можливості прийняття КСЗІ в дослідну експлуатацію.

Попередні випробування проводяться у відповідності з програмою і методиками випробувань. Їх організовує замовник ІТС, а проводить – розробник КСЗІ спільно із замовником.

**7 етап.** Дослідна експлуатація

Під час дослідної експлуатації КСЗІ:

– відпрацьовуються технології захисту оброблюваної інформації, оббіг машинних носіїв інформації, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

– співробітники системи захисту інформації (далі – СЗІ) та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань забезпечення режиму доступу;

– здійснюється доопрацювання програмного забезпечення, додаткове налаштування та конфігурування КЗЗ від НСД;

– здійснюється коригування робочої та експлуатаційної документації.

Дослідна експлуатація ІТС повинна здійснюватися без використання інформації, що становить державну таємницю.

У разі використання в складі КСЗІ комплексу засобів захисту інформації від НСД, який не має експертного висновку про відповідність вимогам НД ТЗІ, необхідно здійснити комплекс робіт з підготовки до проведення оцінки відповідності цього комплексу засобів захисту інформації ви-

могам НД ТЗІ під час проведення державної експертизи КСЗІ.

**8 етап.** Державна експертиза КСЗІ

Комплексна система захисту інформації, що є власністю держави, або інформації з обмеженим доступом, або іншої інформації, захист якої гарантується державою, повинна мати атестат відповідності вимогам захисту інформації, який видається ДССЗЗІ України за результатами державної експертизи.

Державна експертиза КСЗІ проводиться з метою визначення її відповідності технічному завданню, вимогам нормативно-правових актів і нормативних документів щодо захисту інформації та з метою визначення можливості введення КСЗІ в експлуатацію в складі ІТС.

Державна експертиза КСЗІ є етапом приймальних випробувань ІТС та проводиться у відповідності до Положення про державну експертизу в сфері технічного захисту інформації.

Якщо в ІТС обробляється інформація, яка є власністю держави, або інформація, захист якої гарантується державою, то дозвіл на експлуатацію ІТС дається наказом керівника організації тільки за наявності атестату відповідності КСЗІ.

**9 етап.** Супровід КСЗІ

На цьому етапі виконуються роботи з організаційного забезпечення функціонування КСЗІ, її планової модернізації та з управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ. [5]

## 3. РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ

Під політикою безпеки інформації в Системі розуміється набір законів, нормативних документів, вимог, правил, обмежень, інструкцій, рекомендацій, що регламентують порядок обробки інформації і спрямовані на захист інформації від визначених погроз. Політика безпеки розробляється для окремого компонента Системи, послуги захисту і Системи в цілому. Політика безпеки інформації в Системі є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи і положення.[4]

Виходячи з міжнародного досвіду та вимог міжнародних стандартів в області інформаційної безпеки розрізняють три типи ПБ (рис. 2).

Програмна ПБ – є політикою вищої ланки управління в організації. Об'єктом є організація в цілому, за розробку і здійснення програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки (далі – ІБ).

Системно – орієнтована політика – структура, склад, вимоги до етапу документування, які визначені вітчизняними нормативними документами.

Проблемно – орієнтована політика. Об'єктом такої політики є окрема проблема чи завдання в області забезпечення ІБ. Існує ряд областей діяльності організації, для яких необхідно розробити проблемно – орієнтовану політику.

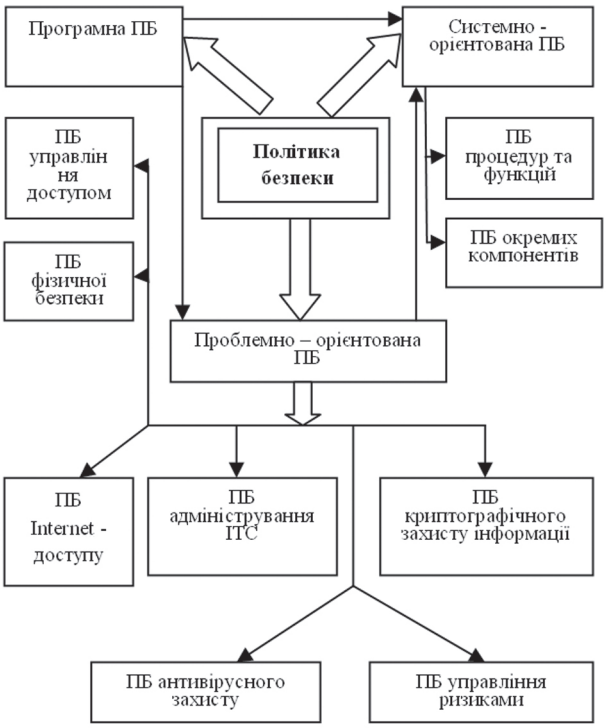


Рис. 2. Типи політики безпеки

Зміст політики безпеки Системи визначається технологією обробки інформації, моделями порушників і погроз, особливостями обчислювальної системи, фізичного середовища й інших факторів. Унаслідок цього, якщо в якій-небудь Системі реалізуються різні технології обробки інформації, то і політика безпеки в такій Системі буде складатися з декількох істотно відмінних частин, кожна з яких буде відповідати конкретної технології обробки інформації. Як складові частини загальної політики безпеки Системи можуть розроблятися політики забезпечення конфіденційності, цілісності, спостережності і доступності оброблюваної інформації, а також правила розмежування доступу (ПРД), що регламентують правила доступу користувачів і процесів до ресурсів Системи.

Політика безпеки повинна передбачати комплексне використання правових і морально-етичних норм, організаційних (адміністративних) мір, фізичних, технічних (апаратних і програмних) способів і засобів захисту інформації, а також визначати правила і порядок їхнього застосування в Системі. Політика безпеки повинна базуватися на принципах системності, комплексності, безперервності захисту, достатності механізмів і заходів захисту і їхньої адекватності погрозам, гнучкості керування системою захисту, простоти і зручності її використання, відкритості алгоритмів і механізмів захисту, якщо інше не передбачене окремо.[3]

Політика безпеки Системи повинна доказово давати гарантії того, що:

– у Системі (у кожній окремій складовій частині, у кожній функціональній задачі) забезпечується адекватність рівня захисту інформації рівню її критичності;

– реалізація заходів захисту інформації є рентабельної;

– у будь-якім середовищі функціонування Системи забезпечується оцінка і перевірка захищеності інформації;

– забезпечується персоніфікація положень політики безпеки (щодо суб'єктів Системи), звітність (реєстрація, аудит) для всіх критичних з погляду безпеки ресурсів, до яких здійснюється доступ;

– персонал і користувачі забезпечені досить повним комплектом документації щодо порядку забезпечення захисту інформації;

– усі критичні з погляду безпеки інформації технології (функції) Системи мають відповідні плани забезпечення безупинної роботи і її поновлення у випадку виникнення непередбачених ситуацій.

Методологія розробки політики безпеки містить у собі наступні роботи:

– розробка концепції безпеки інформації в Системі;

– аналіз ризиків;

– визначення вимог до методів і засобів захисту;

– вибір основних рішень по забезпеченню безпеки інформації;

– організація виконаних робіт і забезпечення безупинного функціонування Системи;

– документальне оформлення політики безпеки.

У загальному випадку документ «Політика безпеки Системи» повинний містити в собі опис:

1. Об’єктів (елементів ресурсів) Системи;
2. Основних погроз інформації;
3. Вимог по захисту від погроз;
4. Принципів керування доступом користувачів до інформації;
5. Правил розмежування інформаційних потоків;
6. Правил маркірування носіїв інформації;
7. Основних атрибутів доступу користувачів, процесів і пасивних об’єктів;
8. Правил розмежування доступу користувачів і процесів до пасивних об’єктів;
9. Правил адміністрування КСЗІ і реєстрації дій користувачів. [7]

У розділі «Опис об’єктів (елементів ресурсів) Системи» на основі інвентаризації (ідентифікації) усіх компонентів Системи, що беруть участь у технологічному процесі обробки інформації, приводиться опис критичних з погляду безпеки активних і пасивних компонентів Системи.

Інвентаризації (ідентифікації) підлягають:

– організаційно-топологічна структура Системи, для якої створюється КСЗІ;

– склад і призначення функціональних підсистем Системи;

– склад служб і протоколів, що реалізують інформаційний обмін між елементами (компонентами) Системи;

– об'єкти захисту (види і категорії оброблюваної інформації, апаратно-програмні й інформаційні ресурси на відповідних рівнях ієрархічної структури Системи);

– персонал і користувачі Системи.

При описі компонентів Системи рекомендується скласти структурну схему інформаційних потоків між основними компонентами Системи, а також описати ( чи формально неформально) технологію обробки інформації. При виборі й аналізі об'єктів Системи важливим моментом є ступінь деталізації розглянутих об'єктів. Так, для Системи 1-го класу (окрема ПЕОМ) припустимо розглядати всю інфраструктуру, тоді як для Системи 3-го класу (глобальна мережа) всеосяжна оцінка може зажадати неприйнятних витрат часу і сил. У цьому випадку рекомендується зосередитися на описі найбільш важливих компонентів Системи.

У розділі «Опис основних погроз інформації» на основі аналізу ризиків приводиться перелік і класифікація можливих видів погроз безпеки інформації в Системі. Під погрозою безпеки розуміються які-небудь чи обставини дії, що можуть бути причиною порушення політики безпеки інформації чи нанесення збитку Системі. Збиток полягає в порушенні якості інформації користувачів (у семантичному і прагматичному змісті) шляхом її знищення, чи зміни несанкціонованого одержання, або в знищенні, чи зміні несанкціонованому використанні ресурсів Системи. У залежності від класу Системи аналіз погроз необхідно здійснювати на рівні окремих апаратних, апаратно-програмних і програмних засобів, окремої локальної обчислювальної мережі, глобальної мережі. Аналіз ризиків передбачає розробку моделі погроз для інформації і моделі порушника, установлення відповідності моделі погроз і об'єктів захисту, оцінку можливості реалізації погрози (оцінка ризику), кількісну або якісну оцінку величини можливого збитку внаслідок реалізації погроз конфіденційності, цілісності, спостережності чи доступності інформації або втрати керованості Системи. Для розробки моделі погроз необхідно сформувати перелік основних погроз і описати можливі способи їхнього здійснення на основі аналізу об'єктів Системи, характеристик обчислювальної системи, фізичного середовища, персоналу, особливостей функціонування Системи.

У розділі «Вимоги по захисту від погроз» приводяться основні задачі і мети захисту інформації, об'єкти захисту, обраний варіант побудови КСЗІ Системи. З урахуванням класу Системи для кожного компонента і Системи в цілому перелічуються функціональні послуги безпеки і вимоги до рівнів реалізації кожної з них, рівень гарантій реалізації послуг. Для кожного компонента і Системи в цілому визначаються загальні підходи і вимоги по захисту інформації від витоку технічними

каналами. На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами. При необхідності визначаються компоненти Системи, для яких доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки Системи. Вихідними даними для розробки вимог по захисту від погроз є задачі і функції Системи, результати аналізу середовища функціонування Системи, модель погроз, модель порушників, результати аналізу ризиків.

У розділі «Опис принципів керування доступом користувачів до інформації» приводяться обраний метод керування доступом (довірче і адміністративне керування), вимоги до забезпечення безперервності захисту, до набору атрибутів доступу і правилам їхнього використання (присвоєння, застосування, зміна, скасування), до реєстрації дій користувачів при використанні ресурсів Системи, а також інших подій, що впливають на дотримання реалізованої в Системі політики безпеки.

У розділі «Опис правил розмежування інформаційних потоків» приводиться перелік інформаційних потоків, що циркулюють між компонентами Системи. У залежності від класу Системи структурна схема інформаційних потоків між основними компонентами Системи може включати:

– внутрішні потоки обміну між активними і пасивними об'єктами усередині однієї ПЕОМ;

– локальні потоки обміну між робочими станціями і серверами усередині однієї ЛОМ (домена);

– міжмережеві потоки обміну між ЛОМ (доменами), що входять до складу однієї Системи;

– потоки обміну інформацією з вилученими взаємодіючими об'єктами, що не входять до складу Системи.

Правила розмежування інформаційних потоків формулюються на основі аналізу області (границі) існування, спрямованості (вхідні чи вихідні), джерел і приймачів, функціонального призначення потоків, вимог по забезпеченню конфіденційності, цілісності, спостережності і доступності. Правила повинні визначати, де і на яких рівнях взаємодії систем повинне здійснюватися розмежування інформаційних потоків і з використанням яких атрибутів і механізмів (ідентифікаторів безпеки, мережних портів, ключів аутентифікації, ключів напрямків і мережних ключів шифрування). Правила повинні також визначати умови й обмеження по ініціюванню і завершенню процесів інформаційного обміну, наприклад, у виді асоціації безпеки.

У розділі «Опис правил маркірування носіїв інформації» приводяться правила, що регламентують порядок обліку, збереження, копіювання, використання і знищення носіїв інформації. Правила формулюються на основі вивчення форм існування критичної інформації на всіх етапах життєвого циклу Системи, середовища функціонування Системи, моделі погроз для інформації і моделі порушників, результатів аналізу ризиків, вимог по забезпеченню конфіденційності, цілісності, спостережності і доступності інформації.

У розділі «Опис основних атрибутів доступу користувачів, процесів і пасивних об'єктів» приводяться склад атрибутів доступу (ідентифікаційні імена, індивідуальні і групові ідентифікатори безпеки, паролі, мітки і /чи маркери доступу, списки контролю доступу), вимоги до характеристик атрибутів доступу (приналежність, унікальність, розмірність, терміни дії) і правила роботи з ними (присвоєння, використання, модифікація, скасування).

У розділі «Опис правил розмежування доступу користувачів і процесів до пасивних об'єктів» міститься набір правил визначальних склад обличчя, яким дозволений доступ до ресурсів Системи, порядок правильного використання ресурсів Системи, статус, права і привілеї адміністратора безпеки Системи, статус, права і привілеї користувачів Системи.

У розділі «Опис правил адміністрування КСЗІ і реєстрації дій користувачів» приводиться порядок адміністрування облікових записів користувачів, профілів користувачів, груп користувачів, загальних ресурсів і аудита.

## 4. РОЗРОБКА ТЕХНІЧНОГО ЗАВДАННЯ

Вимоги до порядку розробки, складу й змісту ТЗ на створення КСЗІ в АС, призначеної для обробки, збереження і передачі інформації досить повно встановлює нормативні документи, згідно з якими ТЗ на КСЗІ в загальному випадку повинно містити такі основні розділи:

– загальні відомості;

– мета і призначення комплексної системи захисту інформації;

– загальна характеристика автоматизованої системи та умов її функціонування;

– вимоги до комплексної системи захисту інформації;

– вимоги до складу проектної та експлуатаційної документації;

– етапи виконання робіт;

– порядок внесення змін і доповнень до ТЗ;

– порядок проведення випробувань комплексної системи захисту інформації. [3]

Розробка ТЗ на комплексну систему захисту інформації являє собою самостійний, досить складний і трудомісткий процес, що включає роботи, основний склад яких виконується на попередньому етапі створення КСЗІ.

Технічне завдання на створення КСЗІ в АС поряд із законодавчими актами, стандартами та нормативними документами ДССЗЗІ України в області захисту інформації є обов'язковим основоположним організаційно-технічним документом при виконанні робіт із забезпечення захисту

інформації в системі, а також під час проведення експертизи АС на відповідність вимогам захищеності інформації. В організаційному аспекті, головне завдання ТЗ на КСЗІ – забезпечити нормативно-технічну базу взаємодії Замовника (власника або користувача АС) КСЗІ, Розробника КСЗІ та експертної організації у процесі розробки, виробництва (впровадження), випробувань, оцінки безпеки інформації та експлуатації КСЗІ.

Для Замовника КСЗІ технічне завдання є документом, що дозволяє на підставі результатів проведеного аналізу ризиків та обраної політики безпеки сформулювати запити до захисту АС у вигляді стандартизованих вимог.

Для Розробника технічне завдання на КСЗІ є керівним документом, що дозволяє на підставі результатів проведеного аналізу запитів Замовника КСЗІ:

– визначити завдання захисту і набір вимог безпеки (функціональних вимог, вимог гарантій та вимог до середовища експлуатації), яким повинна задовольняти, розробляється КСЗІ;

– довести, що вимоги безпеки реалізовані з заданим рівнем гарантій;

– визначити умови, які необхідно виконати для успішного виконання оцінки безпеки інформації готового продукту інформаційної технології.

Для експертної організації ТЗ на КСЗІ є документом, що визначає основні критерії відповідності КСЗІ вимогам Замовника і загрозам, що діють у середовищі експлуатації.

Рівень складності розробки, зміст, вимоги і складові частини ТЗ на КСЗІ визначаються:

– класом, що захищається АС (одномашинний однокористувацький комплекс, локальний багатомашинний багатокористувацький або глобальна мережа);

– організаційно-топологічної структурою;

– способами організації взаємодії між компонентами АС;

– обсягом завдань захисту інформації, сформульованих Замовником (користувачем) АС;

– адекватністю моделі загроз реальних умов експлуатації АС.

Істотну роль відіграють початкові умови розробки ТЗ на КСЗІ – створення захищеного АС з "нуля" або модернізація КСЗІ для існуючої (функціонуючої) АС.

За будь-яких початкових умовах розробка ТЗ на КСЗІ для АС класу 1 (одномашинний однокористувацький комплекс) особливих проблем не викликає внаслідок прозорість всієї інформаційної інфраструктури.

У разі створення захищеної АС з "нуля" при розробці ТЗ на КСЗІ для АС класу 2 (локальний багатомашинний багатокористувацький комплекс) і особливо класу 3 (глобальна мережа) внаслідок того, що ТЗ на КСЗІ і основне ТЗ на АС розробляються паралельно (одночасно) виникає ряд факторів, що впливають на складність розробки, зміст, вимоги і складові частини ТЗ на КСЗІ.

Перший фактор полягає в тому, що загально технічні вимоги (ЗТВ) до архітектури АС (функціональної та організаційно-топологічної структурі, інформаційного, програмного і технічного забезпечення) і розробка вимог до КСЗІ формуються одночасно, внаслідок чого створюється дефіцит часу для розробника ТЗ на КСЗІ. При цьому ЗТВ є вихідними даними для проведення аналізу ризиків, розробки політики безпеки і підрозділу «Загальна характеристика автоматизованої системи та умови її функціонування». Для виключення випадків порушення встановлених строків подання ТЗ Замовнику необхідно при складанні графіка розробки ТЗ враховувати цю особливість і жорстко регламентувати роботу виконавців.

Другий фактор полягає в тому, що класифікація і опис ресурсів АС, розробка інформаційної моделі, аналіз ризиків та розробка політики безпеки проводяться в умовах апріорної невизначеності щодо кінцевих загальних характеристик АС та умов її функціонування тому остаточна архітектура, технічні характеристики та особливості функціонування захищається АС будуть сформовані тільки на стадії ескізно-технічного проектування. Тому за результатами етапів виконаних робіт зі створення захищеної АС технічне завдання на КСЗІ повинно коректуватися з оформленням додатків в тому ж порядку, що й основний документ.

Третій чинник пов'язаний з процедурами аналізу ризиків і розробкою політики безпеки і полягає у виборі та визначення ступеня деталізації розгляду об'єктів інформаційної інфраструктури. Дана обставина обумовлена тим, що всеохоплююча оцінка може зажадати неприйнятних витрат часу і сил. У цьому випадку доцільно зупинитися на деякій рівні деталізації, визначивши найбільш важливі об'єкти, ризики для яких найбільш великі, і погоджуючись з наближеністю підсумкової оцінки.

Для створюваної з «нуля» АС класу 3, складність розробки, зміст, вимоги і складові частини розділів «Мета і призначення комплексної системи захисту інформації» та «Вимоги до комплексної системи захисту інформації» ТЗ на КСЗІ АС визначаються організаційно-топологічною структурою, способами організації взаємодії між компонентами АС, складністю вибору та обґрунтування функціонального профілю захищеності від НСД і вимог до захищеності інформації від витоку технічними каналами.

Дана обставина обумовлена тим, що АС класу 3 (глобальна мережа), як правило, являє собою сукупність складових частин, що є АС класу 2 (локальні багатомашинних багатокористувацькі комплекси) і АС класу 1 (одномашинний однокористувацький комплекси).

АС класу 2 і АС класу 1 можуть об'єднуватися допомогою відомчої виділеної середовища пере-

дачі або через загальнодоступні канали зв'язку (приклад Internet, канали телефонної мережі). В останньому випадку використання служб і механізмів захисту інформації дозволяє будувати віртуальні захищені мережі (VPN).

Кожна складова частина має свою архітектуру, зовнішнє середовище, обслуговуючий персонал та інформаційні технології. Внаслідок цього, в залежності від сформульованих Замовником (користувачем) АС завдань захисту, політики безпеки та умов експлуатації, кожна із складових частин АС класу 3 може відрізнятися від іншої підкласом, складом функціональних послуг безпеки, рівнем гарантій та вимог до захищеності інформації від витоку технічними каналами.

З позицій системного підходу до складу функціональних послуг безпеки окремих складових частин КСЗІ АС класу 3 можуть включатися функції безпеки не притаманні цієї складової частини і забезпечують прояв якого-небудь системного властивості КСЗІ АС класу 3.

Вибір і обґрунтування функціонального профілю захищеності та рівня гарантій окремої складової частини КСЗІ АС класу 3 повинен здійснюватися не тільки на основі її підкласу, але і з урахуванням вимог до загальносистемних послуг безпеки.

Вибір і обґрунтування функціонального профілю захищеності АС класу 3 здійснюється шляхом інтеграції функціонального профілів складових частин з виділенням функціональних послуг безпеки і рівнів гарантій, притаманних КСЗІ.

Зміст розділу «Вимоги до комплексної системи захисту інформації» ТЗ на КСЗІ АС та вимоги до функціональних послуг безпеки істотно залежать від способів утворення захищених віртуальних каналів і вимог замовника за ступенем захищеності інформації, що циркулює у відкритих каналах зв'язку. Дана обставина робить істотний вплив на:

– вибір вимог до функцій і рівнями гарантій криптографічного захисту інформації;

– формування принципів і варіантів організації захищених віртуальних каналів;

– визначення ініціаторів і термінаторів тунелю;

– вибір протоколів тунелювання, методів автентифікації і шифрування.

Для створюваної з «нуля» АС класу 3 зміст розділу «Вимоги до комплексної системи захисту інформації» ТЗ на КСЗІ може включати в якості підрозділів вимоги до функціональних послуг безпеки та рівнями гарантій окремих складових частин (АС першого та другого класів).

Доцільність введення окремих підрозділів для складових частин АС визначається в кожному конкретному випадку залежно від ступеня «неспівпадання» політик безпеки та умов експлуатації, підкласів, складів функціональних послуг безпеки, рівнів гарантій та вимог до захищеності інформації від витоку технічними каналами.

Для розробки ТЗ на КСЗІ АС класу 3 (глобальна мережа) в додаток до функціонального профілю захищеності, обов'язковими вихідними даними повинні бути завдання захисту, політика і концепція безпеки АС, сформовані Замовником (користувачем) АС.

Під завданнями захисту розуміється потреба замовника АС (споживача інформаційної технології) в протистоянні безлічі загроз безпеки або в необхідності реалізації політики безпеки за певних умов експлуатації АС.

Прикладами завдань захисту інформації можуть бути:

– забезпечення певних політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення й експлуатації АС;

– своєчасне виявлення і знешкодження загроз для ресурсів АС, причин та умов, які можуть призвести до порушення її функціонування та розвитку;

– ефективне блокування (попередження) загроз для ресурсів АС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

– управління засобами захисту інформації, керування доступом користувачів до ресурсів АС, контроль за їх роботою з боку персоналу КСЗІ, оперативне сповіщення про спроби НСД до ресурсів АС;

– реєстрація, збір, збереження, обробка даних про всі події в системі, які мають відношення до безпеки інформації.

При виборі і обґрунтуванні задач захисту для кожної складової частини АС третього класу має бути показано, що пропонований склад завдань відповідає параметрам середовища експлуатації, а їх рішення дозволить ефективно протистояти певним загрозам безпеки і реалізувати політику безпеки, визначену для даної складової частини і АС.

Розробка політики і концепції безпеки в АС будь-якого класу повинна передувати розробці ТЗ на створення КСЗІ.

При виборі і обґрунтуванні функціонального профілю захищеності для кожної складової частини АС класу 3 необхідно забезпечити такий рівень деталізації вимог, який дозволяє показати їх відповідність завданням захисту даної АС. При виборі і обґрунтуванні вимог до функціональних послуг безпеки повинні бути дотримані наступні умови:

– сукупність цілей функціональних послуг безпеки повинні відповідати встановленим завданням захисту;

– вимоги безпеки повинні бути узгодженими, тобто не суперечити один одному, а навпаки – взаємно підсилювати.

При розробці ТЗ на модернізацію КСЗІ для існуючої (функціонуючої) АС повинні бути прийняті до уваги причини проведення модернізації.

Необхідність модернізації КСЗІ існуючої АС будь-якого класу може бути обумовлена наступним:

– подальшим розвитком і вдосконаленням існуючої АС;

– зміною Замовником (користувачем) АС завдань захисту інформації;

– появою нових загроз.

У першому випадку особливості розробки ТЗ на модернізацію КСЗІ існуючої АС будь-якого класу аналогічні розробки ТЗ на КСЗІ для АС створюваної з «нуля».

У другому і третьому випадках основна особливість розробки ТЗ на модернізацію КСЗІ існуючої АС будь-якого класу полягає в тому, що в загальному випадку впровадження комплексів засобів захисту (КЗЗ) потребують внести істотні зміни в загальносистемні і технічні характеристики існуючої АС, що пов'язано з фінансовими витратами в додаток до витрат на створення КСЗІ. Тому при формуванні вимог безпеки (функціональних вимог, вимог гарантій та вимог до середовища експлуатації), що забезпечують реалізацію задач захисту, необхідно визначити по можливості повно можливі структурні і технічні зміни в архітектурі існуючої АС, викликані необхідністю досягнення необхідного рівня захищеності, та можливість їх реалізації Замовником [8].

КСЗІ в АС будь-якого класу реалізується комплексним застосуванням методів технічного та криптографічного захисту інформації в автоматизованій системі. Обов'язковим є включення у склад вимог до послуг безпеки (конфіденційність, цілісність, доступність і неспростовність) та рівнями гарантій вимог до функцій і рівнями гарантій криптографічного захисту інформації, наприклад таких, як:

а) управління ключами:

– генерація ключів заданого розміру за певними алгоритмами відповідно до спеціальних стандартами;

– розподіл ключів способами, визначеними в спеціальних стандартах;

– здійснення доступу до ключів з використанням методів, визначених у спеціальних стандартах;

– знищення ключів з використанням методів, визначених у спеціальних стандартах;

б) криптографічні засоби:

– виконання криптографічних операцій з використанням ключів заданого розміру і певних алгоритмів у відповідності зі спеціальними стандартами.

Вимоги до функцій і рівнями гарантій криптографічного захисту інформації в обов'язковому порядку повинні включатися до опису функціонального профілю захищеності, який повинен бути реалізований в АС.

## ВИСНОВКИ

В даній статті особлива увага приділяється передпроектним роботам КСЗІ, а саме: розробці політики безпеки та технічному завданню.

На етапі розробки політики безпеки розробник КСЗІ проводить детальне вивчення об'єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі необхідності додаткові науково-дослідні роботи (НДР), пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися.

Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації.

Політика безпеки залежить від:

– конкретної технології обробки інформації;

– використаних технічних і програмних засобів;

– розташування організації.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.4-001 «Типове положення про службу захисту інформації в інформаційно-телекомунікаційних системах».[7]

В технічному завданні вказуються призначення об'єкта, область його застосування, стадії розробки конструкторської (проектної, технологічної, програмної) документації, її склад, терміни виконання, а також особливі вимоги, зумовлені специфікою самого об'єкту або умовами його експлуатації. Як правило, ТЗ складають на основі аналізу результатів попередніх досліджень, розрахунків і моделювання.

Як інструмент комунікації спілкування замовник-виконавець, технічне завдання дозволяє: обом сторонам:

– представити готовий продукт;

– виконати поетапно перевірку готового продукту (приймальне тестування – проведення випробувань);

– зменшити число помилок, пов'язаних зі зміною вимог в результаті їх неповноти або хибності (на всіх стадіях і етапах створення, за винятком випробувань).

Замовнику:

– усвідомити, що саме йому потрібно;

– вимагати від виконавця відповідності продукту всім умовами, що вказані в ТЗ.

Виконавцю:

– зрозуміти суть завдання, показати замовнику «технічний вигляд» майбутнього виробу, програмного виробу або автоматизованої системи;

– спланувати виконання проекту і працювати за наміченим планом;

– відмовитися від виконання робіт, не зазначених у ТЗ.

**Література.**

[1] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 року, № 2594-IV, К., 2005.

[2] Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005.

[3] *Марущак А.І.* Правові основи захисту інформації з обмеженим доступом: курс лекцій. – К.: КНТ, 2007.-208 с.

[4] *Бондаренко М.Ф., Черних С.П., Горбенко І.Д., Замула А.А., Ткач А.А.* Методические основы концепции и политики безопасности информационных технологий. Радиотехника. 2001. Вып.119.с.5-17.

[5] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. НД ТЗІ 1.1-005-07.

[6] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. НД ТЗІ 3.1-001-07.

[7] Типове положення про службу захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 1.4-001.

[8] Методологічні вказівки щодо розробки ТЗ на створення КСЗІ в АС. НД ТЗІ 3.7-001-99.

Надійшла до редколегії 30.06.2010.

**Землянко Юлія Валеріївна,** асистент кафедри інформаційних технологій ХДУХТ. Область наукових інтересів: наукове обґрунтування напрямків активізації дослідження. Використання у навчальному процесі ігрових методик, відео- та медіа технологій.

**Замула Олександр Андрійович,** професор кафедри БІТ ХНУРЕ, канд. техн. наук, доцент. Область наукових інтересів: технології захисту інформації в інформаційно-телекомунікаційних системах.

**Ткач Александр Александрович,** заместитель главного конструктора ЗАО «Институт информационных технологий». Область научных интересов: безопасность информационных технологий, методология создания и оценки эффективности комплексных систем защиты информации в информационных и информационно-телекоммуникационных системах.

**Литвинова Наталья Ивановна,** студентка кафедры БИТ ХНУРЭ. Область научных интересов: вопросы построения комплексных систем защиты информации в информационно-телекоммуникационных системах.

**Пересичанская Ярослава Андреевна,** студентка кафедры БИТ ХНУРЭ. Область научных интересов: вопросы построения комплексных систем защиты информации в информационно-телекоммуникационных системах.

---

УДК 004.056.5

**Принципы и порядок разработки комплексных систем защиты информации в информационно-телекоммуникационных системах** / Ю.В. Землянко, А.А Замула, А.А. Ткач, Н.И. Литвинова, Я.А. Пересечанская // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 460–469.

Рассматривается порядок осуществления мер и применения средств защиты при создании комплексных систем защиты информации в современных информационно – телекоммуникационных системах.

*Ключевые слова:* комплексные системы защиты информации, информационно-телекоммуникационные системы.

Ил.02. Библиогр.: 08 назв.

UDC 004.056.5

**Principles and order of developing complex information security systems in information and telecommunication systems** / U.V. Zemlyanko, A.A. Zamula, A.A. Tkach, N.I. Litvinova, Y.A. Peresechanskaya // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 460-469.

A procedure for implementing measures and using means to create complex systems of information protection in modern information and telecommunication systems is considered.

*Key words:* complex systems of information protection, information and telecommunications systems.

Fig. 02. Ref.: 08 items.