НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Департамент спеціальних телекомунікаційних систем та
захисту інформації Служби безпеки України

Київ 1999

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту
спеціальних
телекомунікаційних
систем та захисту
інформації Служби
безпеки України
від “ 28 ” квітня 1999 р.
№ 22
із змінами згідно наказу
Адміністрації
Держспецзв'язку від
28.12.2012 № 806

Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

НД ТЗІ 1.1-002-99

ДСТСЗІ СБ України

Київ

Передмова

1 РОЗРОБЛЕНО товариством з обмеженою відповідальністю «Інститут комп'ютерних технологій»

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

3 ВВЕДЕНО ВПЕРШЕ

Зміст

1 Галузь використання 5
2 Нормативні посилання 5
3 Визначення 6
4 Позначення і скорочення 6
5 Постановка проблеми захисту інформації в комп'ютерних системах від несанкціонованого доступу 6
5.1 Загальні положення 6
5.2 Основні напрями захисту 7
6 Концепція забезпечення захисту інформації 10
6.1 Основні загрози інформації 10
6.2 Політика безпеки інформації 11
6.3 Комплекс засобів захисту і об'єкти комп'ютерної системи 12
6.4 Визначення несанкціонованого доступу 13
6.5 Модель порушника 13
7 Основні принципи забезпечення захисту інформації 14
7.1 Планування захисту і керування системою захисту 14
7.2 Основні принципи керування доступом 15
7. 2.1 Безперервний захист 15
7. 2. 2 Атрибути доступу 15
7. 2. 3 Довірче і адміністративне керування доступом 16
7.2.4 Забезпечення персональної відповідальності 17
7.3 Послуги безпеки 18
7.4 Гарантії 18
8 Основні принципи реалізації програмно-технічних засобів 18
8.1 Функції і механізми захисту 18
8.2 Реалізація комплексу засобів захисту 19
8.3 Концепція диспетчера доступу 20

НД ТЗІ 1.1-002-99

ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Чинний від

1999-07-01

1 Галузь використання

Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

- визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;
- створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. д.) критичної інформації (інформації, що вимагає захисту), а також для державних органів, що здійснюють функції контролю за обробкою такої інформації.

Необхідно визнати, що на сьогоднішній день проблема захисту інформації не має остаточного вирішення. Тому цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З часом, як наслідок практичного застосування, а також з появою і розвитком нових тенденцій і підходів, в цей нормативний документ і інші нормативні і методологічні документи, що на ньому базуються, будуть вноситися відповідні корективи.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

- Закон України “Про інформацію”;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України “Про науково-технічну інформацію”;
- Закон України “Про державну таємницю";
- Концепція (основи державної політики) національної безпеки України;
- Концепція технічного захисту інформації в Україні;
- Положення про порядок здійснення криптографічного захисту інформації в Україні;

- НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

3 Визначення

В цьому НД ТЗІ використовуються терміни і визначення, що відповідають встановленим нормативним документом ТЗІ 1.1-003-99 “Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу”.

4 Позначення і скорочення

У цьому НД ТЗІ використовуються такі позначення і скорочення:

АС — автоматизована система;

БД — база даних;

ЕОМ — електронно-обчислювальна машина;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД — нормативний документ;

НД СТЗІ — нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОС — обчислювальна система;

ПЕМВН — побічні електромагнітні випромінювання і наводи;

ПЗ — програмне забезпечення;

ПЗП — постійний запам’ятовуючий пристрій;

ПРД — правила розмежування доступу;

ТЗІ — технічний захист інформації.

5 Постановка проблеми захисту інформації в комп'ютерних системах від несанкціонованого доступу

5.1 Загальні положення

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів. Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються несприятливими. Потенційно можливий несприятливий вплив називається загрозою.

Захист інформації, що обробляється в АС, полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації і АС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і АС, що

її обробляє. Система зазначених заходів, що забезпечує захист інформації в АС, називається комплексною системою захисту інформації.

Істотна частина проблем забезпечення захисту інформації в АС може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту.

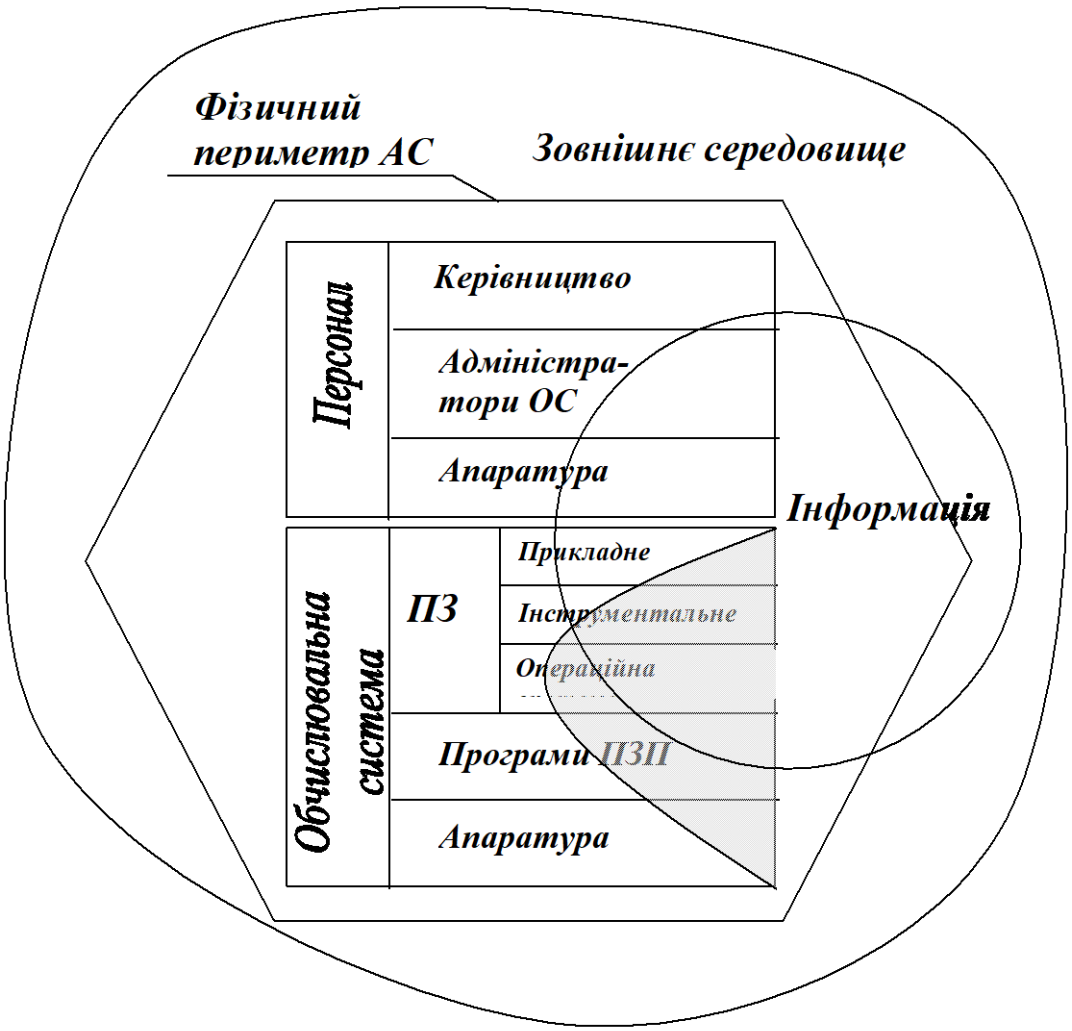
Правовою основою забезпечення технічного захисту інформації в Україні є Конституція України, Закони України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про державну таємницю", "Про науково-технічну інформацію", Концепція (основи державної політики) національної безпеки України, Концепція технічного захисту інформації в Україні, інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

5.2 Основні напрями захисту

Автоматизована система являє собою організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію (малюнок). Прийнято розрізняти два основних напрями ТЗІ в АС — це захист АС і оброблюваної інформації від несанкціонованого доступу і захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наводів).

Цей документ і комплект НД, що базується на ньому, присвячений питанням організації захисту від НСД і побудови засобів захисту від НСД, що функціонують у складі обчислювальної системи АС. Організаційні і фізичні заходи захисту, включаючи захист від фізичного НСД до компонентів ОС, як і захист від витоку технічними каналами не є предметом розгляду[1]. Незважаючи на це, при викладі увага приділяється також і деяким нетехнічним аспектам, але тільки там, де це впливає на оцінку технічної захищеності.

[1] Порядок захисту від ПЕВМН регламентується окремим комплектом нормативних документів.



- Комплекс засобів захисту

З точки зору методології в проблемі захисту інформації від НСД слід виділити два напрями:

забезпечення і оцінка захищеності інформації в АС, що функціонують;

реалізація та оцінка засобів захисту, що входять до складу компонентів, з яких будується обчислювальна система АС (програмних продуктів, засобів обчислювальної техніки і т. ін.), поза конкретним середовищем експлуатації.

Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її обробки в АС. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу АС, на всіх технологічних етапах обробки інформації і в усіх режимах функціонування. Життєвий цикл АС включає розробку, впровадження, експлуатацію та виведення з експлуатації.

У випадку, якщо в АС планується обробка інформації, порядок обробки і захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформація, що становить державну таємницю), то для обробки такої інформації в цій АС необхідно мати дозвіл відповідного

уповноваженого державного органу. Підставою для видачі такого дозволу є висновок експертизи АС, тобто перевірки відповідності реалізованої КСЗІ встановленим нормам.

Якщо порядок обробки і захисту інформації не регламентується законодавством, експертиза може виконуватись в необов'язковому порядку за поданням замовника (власника АС або інформації).

В процесі експертизи оцінюється КСЗІ АС в цілому. В тому числі виконується і оцінка реалізованих в ОС АС засобів захисту. Засоби захисту від НСД, реалізовані в обчислювальній системі, слід розглядати як підсистему захисту від НСД у складі КСЗІ. Характеристики фізичного середовища, персоналу, оброблюваної інформації, організаційної підсистеми істотно впливають на вимоги до функцій захисту, що реалізуються ОС.

Обчислювальна система автоматизованої системи являє собою сукупність апаратних засобів, програмних засобів (в тому числі програм ПЗП), призначених для обробки інформації. Кожний з компонентів ОС може розроблятись і надходити на ринок як незалежний продукт. Кожний з цих компонентів може реалізовувати певні функції захисту інформації, оцінка яких може виконуватись незалежно від процесу експертизи АС і має характер сертифікації. За підсумками сертифікації видається сертифікат відповідності реалізованих засобів захисту певним вимогам (критеріям). Наявність сертифіката на обчислювальну систему АС або її окремі компоненти може полегшити процес експертизи АС.

Як в процесі експертизи, так і сертифікації оцінка реалізованих функцій захисту інформації виконується відповідно до встановлених критеріїв. Ці критерії встановлюються НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу " (далі — Критерії). З метою уніфікації критеріїв і забезпечення можливості їх застосування як в процесі експертизи АС (тобто оцінки функцій захисту інформації, реалізованих ОС автоматизованої системи, що реально функціонують), так і в процесі сертифікації програмно-апаратних засобів поза конкретним середовищем експлуатації, обидві ці категорії об'єднуються поняттям комп'ютерна система. Під КС слід розуміти представлену для оцінки сукупність програмно-апаратних засобів[2] .

Як КС можуть виступати: ЕОМ загального призначення або персональна ЕОМ; операційна система; прикладна або інструментальна програма (пакет програм); КЗЗ, що окремо поставляється, або підсистема захисту від НСД, наприклад, мережа, яка являє собою надбудову над ОС; локальна обчислювальна мережа, як сукупність апаратних засобів, ПЗ, що реалізує протоколи взаємодій, мережевої операційної системи і т. ін., ОС автоматизованої системи, яка реально функціонує, в найбільш загальному випадку – сама АС або її частина.

---

[2] Термін "комп'ютерна система" аналогічний таким термінам: "computer system", що використовується в "Оранжевій книзі"; "computer product" — у Канадских Критеріях; "target of evaluation" (TOE) — в Європейських Критеріях

Як і в НД ТЗІ 2.5-004-99, далі використовується термін КС. Якщо необхідно підкреслити певні специфічні моменти, безпосередньо зазначається, стосується викладене АС (обчислювальної системи АС) чи сукупності програмно-апаратних засобів, що окремо постачаються, які розглядаються поза конкретним оточенням.

Можлива ситуація, коли для побудови певної КС використовуються компоненти, кожний або деякі з них мають сертифікат, що підтверджує, що ці компоненти реалізують певні функції захисту інформації. Це, однак, не означає, що КС, яка складається з таких компонентів, буде реалізовувати всі ці функції. Для гарантії останнього має бути виконано проектування КС з метою інтеграції засобів захисту, що надаються кожним компонентом, в єдиний комплекс засобів захисту. Таким чином, наявність сертифіката слід розглядати як потенційну можливість КС реалізовувати певні функції захисту оброблюваної інформації від певних загроз.

6 Концепція забезпечення захисту інформації

6.1 Основні загрози інформації

Інформація в КС існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки. Тут і далі під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. (ДСТУ 2226-93). Далі терміни «інформація» і «дані« використовуються як синоніми.

Інформація для свого існування завжди вимагає наявності носія. Як носій інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

При аналізі проблеми захисту від НСД інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення). Інформація зберігає

доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

Загрози можуть впливати на інформацію не безпосередньо, а опосередковано. Наприклад, втрата КС керованості може призвести до нездатності КС забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації.

6.2 Політика безпеки інформації

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення "політика безпеки інформації" може використовуватись словосполучення "політика безпеки", а замість словосполучення "політика безпеки інформації, що реалізується послугою" — "політика послуги" і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

6.3 Комплекс засобів захисту і об'єкти комп'ютерної системи

Комп'ютерна система, як правило, складається з безлічі компонентів. Деякі з компонентів можуть бути спеціально призначені для реалізації політики безпеки (наприклад, засоби ізоляції процесів або керування потоками інформації). Інші можуть впливати на безпеку опосередковано, наприклад, забезпечувати функціонування компонентів першого типу. І, нарешті, треті можуть взагалі не бути задіяні під час вирішення завдань забезпечення безпеки. Множина всіх компонентів перших двох типів називається комплексом засобів захисту.

Іншими словами, КЗЗ — це сукупність всіх програмно-апаратних засобів, в тому числі програм ПЗП, задіяних під час реалізації політики безпеки. Частина КС, що складає КЗЗ, визначається розробником. Будь-який компонент КС, який внаслідок якого-небудь впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина КЗЗ.

Комплекс засобів захисту розглядає ресурси КС як об'єкти і керує взаємодією цих об'єктів відповідно до політики безпеки інформації, що реалізується. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне (форма, синтаксис). Об'єкт характеризується своїм станом, що в свою чергу характеризується атрибутами і поводженням, яке визначає способи зміни стану. Для різних КС об'єкти можуть бути різні. Наприклад, для СУБД в якості об'єктів можна розглядати записи БД, а для операційної системи — процеси, файли, кластери, сектори дисків, сегменти пам'яті і т. ін. Все, що підлягає захисту відповідно до політики безпеки, має бути визначено як об'єкт.

При розгляді взаємодії двох об'єктів КС, що виступають як приймальники або джерела інформації, слід виділити пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію. Далі розглядаються такі типи об'єктів КС: об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти. Прийнятий у деяких зарубіжних документах термін "суб'єкт" є суперпозицією об'єкта-користувача і об'єкта-процеса.

Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного домену — ізольованої логічної області, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини. В інших доменах об'єкти залишаються в пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим об'єктом-процесом або навіть об'єктом-користувачем, оскільки останній залишається "пасивним" з точки зору керуючого об'єкта. Іншими словами, об'єкти можуть знаходитись в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт. Перехід між станами означає, що об'єкт просто розглядається в іншому контексті.

Пасивний об'єкт переходить в стан об'єкта-користувача, коли індивід (фізична особа-користувач) «входить» в систему. Цей об'єкт-користувач виступає для КЗЗ як образ фізичного користувача. Звичайно, за цим процесом іде

активізація об'єкта-процесу за ініціативою користувача. Цей об'єкт-процес є керуючим для пасивних об'єктів всередині домену користувача. Об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти далі позначаються просто як користувачі, процеси і об'єкти, відповідно.

Взаємодія двох об'єктів КС (звернення активного об'єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об'єктами і/або зміни стану системи. Як потік інформації розглядається будь-яка порція інформації, що передається між об'єктами КС.

6.4 Визначення несанкціонованого доступу

Під НСД слід розуміти доступ до інформації з використанням засобів, включених до складу КС, що порушує встановлені ПРД. Несанкціонований доступ може здійснюватися як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу КС розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

- безпосереднє звертання до об'єктів з метою одержання певного виду доступу;
- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє здійснити НСД;
- впровадження в КС програмних або апаратних механізмів, що порушують структуру і функції КС і дозволяють здійснити НСД.

Під захистом від НСД, звичайно, слід розуміти діяльність, спрямовану на забезпечення додержання ПРД шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації. Поняття (термін) захист від НСД є сталим і тому використовується в цьому НД і документах, що на ньому базуються. Проте зміст даного поняття дещо вужчий, ніж коло питань, що розглядаються. Так, політика безпеки КС може містити вимоги щодо забезпечення доступності інформації, які, наприклад, регламентують, що КС має бути стійка до відмов окремих компонентів. Цю вимогу не можна віднести до ПРД, проте її реалізація здійснюється засобами, що входять до складу КЗЗ. Тому система НД щодо захисту інформації в КС від НСД охоплює коло питань, пов'язаних з створенням і підтримкою в дієздатному стані системи заходів, що спрямовані на забезпечення додержання вимог політики безпеки інформації під час її обробки в КС.

6.5 Модель порушника

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник — це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

7 Основні принципи забезпечення захисту інформації

7.1 Планування захисту і керування системою захисту

Для забезпечення безпеки інформації під час її обробки в АС створюється КСЗІ, процес управління якою повинен підтримуватись протягом всього життєвого циклу АС. На стадії розробки метою процесу управління КСЗІ є створення засобів захисту, які могли б ефективно протистояти ймовірним загрозам і забезпечували б надалі дотримання політики безпеки під час обробки інформації. На стадії експлуатації АС метою процесу управління КСЗІ є оцінка ефективності створеної КСЗІ і вироблення додаткових (уточнюючих) вимог для доробки КСЗІ з метою забезпечення її адекватності при зміні початкових умов (характеристик ОС, оброблюваної інформації, фізичного середовища, персоналу, призначення АС, політики безпеки і т. ін.).

На кожному етапі мають бути виконані збирання і підготовка даних, їх аналіз і прийняття рішення. При цьому результати виконаного на певному етапі аналізу і прийняті на їх підставі рішення нарівні з уточненими вимогами слугують вихідними даними для аналізу на наступному етапі. На будь-якій стадії або будь-якому етапі може постати необхідність уточнення початкових умов і повернення на більш ранні етапи.

Створення КСЗІ має починатись з аналізу об'єкта захисту і можливих загроз. Передусім мають бути визначені ресурси АС, що підлягають захисту. Загрози мають бути визначені в термінах ймовірності їх реалізації і величини можливих збитків. На підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики. Ризик являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. Величина ризику може бути виражена в грошовому вимірі або у вигляді формальної оцінки

(високий, низький і т. ін.). На підставі виконаної роботи мають бути вироблені заходи захисту, перетворення яких в життя дозволило б знизити рівень остаточного ризику до прийнятного рівня. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

На підставі проведеного аналізу ризиків сформульованої політики безпеки розробляється план захисту, який включає в себе опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу АС. Вартість заходів щодо захисту інформації має бути адекватною розміру можливих збитків.

7.2 Основні принципи керування доступом

7. 2.1 Безперервний захист

Захист інформації повинен забезпечуватись протягом всього періоду її існування. З моменту створення об'єкта КС або його імпорту до системи і аж до його знищення або експорту з системи всі запити на доступ до об'єкта і об'єкта на доступ до інших об'єктів мають контролюватися КЗЗ.

Перший аспект, що випливає з цього принципу, — це необхідність того, щоб абсолютно всі запити на доступ до об'єктів контролювались КЗЗ і не існувало можливості обминути цей контроль (одержати доступ в обхід КЗЗ). Для захисту об'єктів КЗЗ повинен в першу чергу забезпечувати свою цілісність і керованість.

Другим аспектом є те, що особливе значення набуває визначення діючих за умовчанням правил, які визначають початкові умови, за яких починається існування об'єкта всередині КС.

7. 2. 2 Атрибути доступу

Для реалізації політики безпеки КЗЗ повинен забезпечити ізоляцію об'єктів всередині сфери управління і гарантувати розмежування запитів доступу і керування потоками інформації між об'єктами. Для цього з об'єктами КС має бути пов'язана інформація, що дозволяла б КЗЗ ідентифікувати об'єкти і перевіряти легальність запитів доступу. Як така інформація є атрибути доступу.

Кожний об'єкт КС повинен мати певний набір атрибутів доступу, який включає унікальний ідентифікатор та іншу інформацію, що визначає його права доступу і/або права доступу до нього. Атрибут доступу — термін, що використовується для опису будь-якої інформації, яка використовується при керуванні доступом і зв'язана з користувачами, процесами або пасивними об'єктами. Відповідність атрибутів доступу і об'єкта може бути як явною, так і неявною. Атрибути доступу об'єкта є частиною його подання в КС.

Коли користувачі або процеси намагаються одержати доступ до пасивних об'єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть "прийняти рішення" про легальність запиту. Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати довірче керування доступом, адміністративне, контроль за цілісністю та інші види керування доступом.

Для відображення функціональності КС у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Матриця доступу

являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об'єктів КС, а в якості елементів матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двомірною (наприклад, користувачі/пасивні об'єкти або процеси/пасивні об'єкти) або тримірною (користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих на даний час об'єктів КС даного типу, або частковою. Повна тримірна матриця доступу дозволяє точно описати, хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об'єкта), який вид доступу може одержати.

7. 2. 3 Довірче і адміністративне керування доступом

Під довірчим керуванням доступом слід розуміти таке керування, при якому засоби захисту дозволяють звичайним користувачам управляти (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами), тобто призначення і передача повноважень не вимагають адміністративного втручання.

Адміністративне керуванням доступом — це таке керування, при якому засоби захисту дозволяють управляти потоками інформації між користувачами і об'єктами тільки спеціально авторизованим користувачам. Прикладом реалізації адміністративного керуванням доступом може служити механізм, коли у вигляді атрибутів доступу використовуються мітки, що відображають міру конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином, КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що запитує інформацію, авторизованим користувачем.

Система, що реалізує адміністративне керування доступом, повинна гарантувати, що потоки інформації всередині системи установлюються адміністратором і не можуть бути змінені звичайним користувачем. З іншого боку, система, що реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в т. ч. створювати нові потоки інформації всередині системи.

Створення додаткових потоків інформації може бути зумовлене: модифікацією атрибутів доступу користувача, процесу або пасивного об'єкта; створенням нових об'єктів (включаючи копіювання існуючих); експортом або імпортом об'єктів.

Сталість атрибутів доступу

Якщо система реалізує адміністративне керування доступом, то звичайний користувач не повинен мати можливості ні за яких умов змінювати атрибути доступу об'єкта. Таким чином, якщо політика потоків інформації, створена адміністратором, визначає, що два користувача не можуть розділяти (спільно використовувати) інформацію, то жоден з них не спроможний передати іншому користувачеві свої повноваження щодо доступу до існуючого об'єкта.

І навпаки, система, що реалізує довірче керування доступом, може, наприклад, відповідно до політики безпеки надати звичайному користувачеві можливість змінювати атрибути доступу об'єкта, що належить йому.

Створення нових об'єктів

Якщо система реалізує адміністративне керування доступом і політика потоків інформації, створена адміністратором, визначає, що два користувачі не можуть розділяти інформацію, то жоден з них не повинен бути спроможний створити об'єкт, доступний іншому. Додатково повинні існувати правила для визначення (завдання) атрибутів доступу, що мають присвоюватись об'єкту, одержаному копіюванням існуючого.

І навпаки, система, що реалізує довірче керування доступом, може відповідно до політики безпеки надати звичайному користувачеві можливість влаштовувати атрибути доступу для знову створеного об'єкту. Наприклад, система може дозволяти творцю об'єкта зазначати користувачів, що можуть мати права доступу до об'єкта.

Експорт і імпорт об'єктів

Якщо система реалізує адміністративне керування доступом, то атрибути доступу об'єкта мають зберігатись під час його експорту на зовнішній носій. Додатково повинні існувати правила для присвоєння атрибутів доступу імпортованому об'єкту.

І навпаки, система, що реалізує довірче керування доступом, може надати можливість експортувати об'єкт без збереження атрибутів доступу. Додатково може існувати можливість імпорту звичайним користувачем об'єкта з наступним присвоєнням йому атрибутів доступу на розсуд користувача. Проте, навіть відповідно до політики довірчого керування доступом, атрибути доступу об'єкта під час виконання деяких операцій, наприклад, під час його резервного копіювання, мають зберігатися. Якщо об'єкт буде коли-небудь відновлено з резервної копії, то його атрибути доступу також мають бути відновлені.

7.2.4 Забезпечення персональної відповідальності

Кожний співробітник з персоналу АС має бути ознайомлений з необхідними положеннями політики безпеки і нести персональну відповідальність за їх додержання. Політика безпеки повинна установлювати обов'язки співробітників, особливо тих, що мають адміністративні повноваження, і види відповідальності за невиконання цих обов'язків. Як правило, це забезпечується в рамках організаційних заходів безпеки.

Однак, коли користувач працює з КС, то система розглядає його не як фізичну особу, а як об'єкт, якому притаманні певні атрибути і поводження. Для забезпечення ефективності організаційних заходів необхідна підтримка з боку програмно-апаратних засобів. Комплекс засобів захисту КС повинен забезпечувати реєстрацію дій об'єктів-користувачів щодо використання ресурсів системи, а також інших дій і подій, які так або інакше можуть вплинути на дотримання реалізованої КС політики безпеки.

Система повинна надавати користувачам, що мають адміністративні повноваження, можливість проглядати та аналізувати дані реєстрації, що представляються у вигляді журналів реєстрації, виявляти небезпечні з точки зору політики безпеки події, встановлювати їх причини і користувачів, відповідальних за порушення політики безпеки.

7.3 Послуги безпеки

З точки зору забезпечення безпеки інформації КС або КЗЗ можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз.

Існує певний перелік послуг, які на підставі практичного досвіду визнані "корисними" для забезпечення безпеки інформації. Вимоги до реалізації даних послуг наведені в НД ТЗІ 2.5-004-99. Вимоги до функціональних послуг розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного з чотирьох основних типів: конфіденційності, цілісності, доступності та спостереженості.

Згідно з Критеріями, кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. Для кожної послуги повинна бути розроблена політика безпеки, яка буде реалізована КС. Політика безпеки має визначати, до яких об'єктів застосовується послуга. Ця визначена підмножина об'єктів називається захищеними об'єктами відносно даної послуги.

7.4 Гарантії

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в КС, Критерії містять критерії гарантій, які дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, випробування КЗЗ, середовища функціонування і експлуатаційної документації. В Критеріях вводиться сім рівнів гарантій, які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру упевненості в тому, що послуги, які надаються, дозволяють протистояти певним загрозам, а механізми, що їх реалізують, в свою чергу, коректно реалізовані, і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації КС.

Гарантії забезпечуються як в процесі розробки, так і в процесі оцінки. В процесі розробки гарантії забезпечуються діями розробника щодо забезпечення правильності (коректності) розробки. В процесі оцінки гарантії забезпечуються шляхом перевірки додержання розробником вимог Критеріїв, аналізу документації, процедур розробки і постачання, а також іншими діями експертів, які проводять оцінку.

8 Основні принципи реалізації програмно-технічних засобів

8.1 Функції і механізми захисту

Основними завданнями засобів захисту є ізоляція об'єктів КС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання. З одного боку, будь-яка елементарна функція будь-якої з послуг, що реалізуються засобами захисту, може бути

віднесена до функцій ізоляції, перевірки або реєстрації. З іншого боку, будь-яка з функцій, що реалізуються засобами захисту, може бути віднесена до функцій забезпечення конфіденційності, цілісності і доступності інформації або керованості КС і спостереженості дій користувачів.

Кожна функція може бути реалізована одним або більше внутрішніми механізмами, що залежать від конкретної КС. Водночас одні й ті ж самі механізми можуть використовуватись для реалізації кількох послуг. Наприклад, для розробника слушно реалізувати і адміністративне і довірче керування доступом єдиним набором механізмів.

Реалізація механізмів може бути абсолютно різною. Для реалізації функцій захисту можуть використовуватись програмні або апаратні засоби, криптографічні перетворення, різні методи перевірки повноважень і т. ін. Вибір методів і механізмів практично завжди залишається за розробником. Єдиною вимогою залишається те, щоб функції захисту були реалізовані відповідно до декларованої політики безпеки і вимог гарантій.

Для реалізації певних послуг можуть використовуватись засоби криптографічного захисту. Криптографічні перетворення можуть використовуватись безпосередньо для захисту певної інформації (наприклад, при реалізації послуг конфіденційності) або підтримувати реалізацію послуги (наприклад, при реалізації послуги ідентифікації і автентифікації). Згідно із аконодавством створення переліку вимог, сертифікація і атестація систем шифрування покладається на відповідний уповноважений орган виконавчої влади. Ця діяльність регламентується “Положенням про порядок здійснення криптографічного захисту інформації в Україні”.

8.2 Реалізація комплексу засобів захисту

До реалізації КЗЗ пред'являється ряд вимог.

По-перше, КЗЗ повинен забезпечувати безперервний захист об'єктів КС. Не повинно існувати можливості одержати доступ до об'єктів КС в обхід КЗЗ. КЗЗ, що реалізує політику безпеки, має бути безперервно захищений від злому і несанкціонованої модифікації. Жодна КС, що реалізує функції захисту, не може вважатись такою, якщо базові апаратні і програмні механізми, що реалізують політику безпеки, самі є суб'єктами для несанкціонованої модифікації або заміни.

По-друге, КЗЗ повинен мати модульну структуру. На рівні розгляду архітектури КС "модульність" означає, що КЗЗ має бути реалізований як набір відносно незалежних частин. Кожна з цих частин повинна взаємодіяти з іншими тільки через добре визначені інтерфейси. На рівні розгляду архітектури КЗЗ "модульність" означає, що КЗЗ має бути спроектовано як набір логічних груп програмного і апаратного забезпечення так, щоб кожна група вирішувала певні завдання. Для ПЗ, наприклад, в простішому випадку під цим слід розуміти, що подібні функції мають бути зосереджені в певних вихідних файлах. Під жорсткішими вимогами слід розуміти використання приховання даних, інкапсуляції та інших механізмів, що дозволяють мати впевненість, що кожний модуль вирішує єдине завдання і що всі дані, якими він оперує, або визначені

всередині і доступні як локальні, або передаються як параметри або схожим чином. Будь-яка взаємодія між компонентами повинна здійснюватись тільки через відомі і описані канали (інтерфейси). Оскільки не в усіх випадках це можливо, то за умови забезпечення відповідних гарантій реалізації використання глобальних змінних допускається, хоч і не рекомендується. Посилення вимог до модульності КЗЗ приводить до необхідності побудови КЗЗ відповідно до принципів пошарової архітектури: КЗЗ має бути спроектовано як набір груп функцій (шарів), що взаємодіють тільки з сусідніми нижнім і верхнім шарами.

8.3 Концепція диспетчера доступу

При реалізації КЗЗ використовується концепція диспетчера доступу. Ця концепція не єдино можливий метод, проте є найбільш опрацьованою теоретично і перевіреною на практиці.

Диспетчер доступу характеризується трьома атрибутами:

- забезпечує безперервний і повний захист;
- достовірний (захищений від модифікації);
- має невеликі розміри.

Це означає, що диспетчер доступу має бути завжди активним і повинен контролювати всі запити на доступ до будь-якого захищеного об'єкта, який піддається впливу. Диспетчер доступу має бути захищений від модифікації, що для програмної реалізації звичайно вважається ізоляцією домену КЗЗ від доменів інших процесів. І, нарешті, диспетчер доступу повинен мати невеликі розміри, щоб код (реалізація) був зрозумілим і його можна було перевірити в процесі оцінки. Термін "невеликий" (або "мінімізований ") є відносним. На практиці це означає, що диспетчер доступу не повинен складати весь КЗЗ, а повинен включати мінімально необхідний набір механізмів, що безпосередньо реалізують перевірку легальності запитів на доступ і, можливо, реєстрацію цих запитів.

Головна мета диспетчера доступу — забезпечення відомої точки проходження всіх запитів всередині КС і досягнення гарантії того, що потоки інформації між об'єктами-користувачами, об'єктами-процесами і пасивними об'єктами відповідають вимогам політики безпеки.

Класичний погляд на диспетчер доступу полягає в тому, що він служить бар'єром між інформацією, до якої хоче одержати доступ користувач, і самим користувачем. Диспетчер доступу дозволяє або забороняє доступ відповідно до того, чи є запит авторизованим. Рішення приймається на підставі перевірки атрибутів доступу користувача, процесу і пасивного об'єкта.

Узагальненням концепції диспетчера доступу є ідея герметизації, коли кожний об'єкт як би герметизовано диспетчером доступу, що утворює навкруги нього непроникну оболонку. Кількість захищених (що знаходяться всередині оболонки) об'єктів може вар’юватись від одного об'єкта до всіх об'єктів системи. Таке подання є розширенням класичного підходу для розподілених і об'єктно-орієнтованих систем.

Методи реалізації концепції диспетчера доступу можуть бути різними. Незалежно від реалізації диспетчер доступу повинен забезпечити неможливість доступу до об'єкта в обхід механізмів захисту, перевірку наявності у користувача

і/або процесу прав доступу до об'єкта і реєстрації подій, що відбуваються. Найбільш широке розповсюдження одержала реалізація класичного погляду на диспетчер доступу, яка називається "ядром захисту".