УДК 681.322

Ігор Олександрович Ляшенко

АНАЛІЗ ВИМОГ КЕРІВНИХ ДОКУМЕНТІВ ДЕРЖТЕХКОМІССІЇ РОСІЇ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ

Постановка проблеми. Аналіз останніх досліджень і публікацій

На сучасні інформаційно-управляючі системи покладається вирішення найрізноманітніших та найважливіших завдань: автоматизоване управління технологічними процесами та промисловими підприємствами, автоматизація діяльності банків, управління повітряним рухом, морська та космічна навігація та інше. Інформатизація пронизує всі сфери сучасного суспільства. Вона перетворилась в глобальний, невичерпний ресурс людства, яке вступило в нову епоху розвитку – епоху інформаційної цивілізації.

Завдяки цим процесам відбувається бурхливий розвиток і військової справи. З'являються нові види озброєння, які засновані на застосуванні інформаційних технологій. Розвиваються засоби розвідки, автоматизовані системи управління військами та зброєю. Основу реалізації інформаційних технологій у військовій справі складають інформаційно-управляючі системи.

В Збройних Силах України, не дивлячись на складне становище з фінансування процесу розробки та впровадження автоматизованих систем управління військами та зброєю, триває процес інформатизації. Створюються автоматизовані системи інформаційного, інформаційно-аналітичного та інших видів забезпечення, автоматизовані системи управління військами та зброєю, які мають тенденцію об'єднання у регіональні, корпоративні, а в майбутньому і в глобальну мережу. Вони пронизують усю вертикаль системи управління військами від президента України – Верховного Головнокомандувача ЗС України – до окремої військової частини. При цьому, вже зараз деякі мережі мають точки доступу до всесвітньої глобальної мережі Інтернет.

Відповідно для створення таких систем необхідно мати обґрунтовані стандарти інформаційної безпеки. Головне завдання стандартів інформаційної безпеки — створити основу взаємодії між виробниками, споживачами і експертами по кваліфікації продуктів інформаційних технологій. Відповідно перед стандартами інформаційної безпеки стоїть непросте завдання — примирити точки зору усіх зацікавлених сторін та створити ефективний механізм взаємодії між ними.

Формулювання мети статті. Виклад основного матеріалу

Пропонується проаналізувати основні світові стандарти інформаційної безпеки, зіставити їх структуру, вимоги, що містяться в них, та критерії, а також оцінити ефективність їх практичного застосування на прикладі керівних документів Держтехкомісії Росії. При цьому огляд керівних документів будується за наступною схемою: мета розробки, основні положення, таксономія та ранжирування вимог і критеріїв.

Основні положення.

У 1992 році Держтехкомісія (ДТК при Президентові Російської федерації (РФ) опублікувала п'ять Керівних документів, присвячених питанням захисту від несанкціонованого доступу до інформації ("Концепция защиты средств вычислительной техники от несанкционированного доступа к информации", "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации", "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", "Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники", "Защита от несанкционированного доступа к информации. Термины и определения").

Розглянемо найважливіші з них: "Концепція захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації", "Засоби обчислювальної техніка. Захист від несанкціонованого доступу до інформації. Показники захищеності від несанкціонованою доступу до інформації", "Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем і вимоги до захисту інформації".

Ідейною основою цих документів є "Концепція захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації (НСД)",

що містить систему поглядів ДТК на проблему інформаційної безпеки та основні принципи захисту комп'ютерних систем. З точки зору розробників цих документів основне і чи не єдине завдання засобів безпеки - забезпечення захисту від несанкціонованого доступу (НСД) до інформації. Якщо засобам контролю та забезпечення цілісності ще приділяється деяка увага, то підтримка працездатності систем обробки інформації (як ступінь захисту від загроз працездатності) взагалі не згадується. Певний ухил у бік підтримки секретності пояснюється тим що ці документи були розроблені з розрахунку на застосування в інформаційних системах міністерства оборони та спецслужб РФ, а також недостатньо високим рівнем інформаційних технологій цих систем у порівнянні з сучасним.

Таксономія критеріїв і вимог безпеки.

Керівні документи ДТК пропонують дві групи критеріїв безпеки - показники захищеності засобів обчислювальної техніки (ЗОТ) від НСД та критерії захищеності автоматизованих систем (АС) обробки даних.

Перша група дозволяє оцінити ступінь захищеності (правда тільки відносно загроз одного типу — НСД) компонентів ОС, що окремо поставляються споживачеві, а друга розрахована на повнофункціональні системи обробки даних.

Оскільки ці документи легко доступні та часто служили об'єктами коментарів і критики [1], обмежимося тільки коротким оглядом їх основних положень.

Показники захищеності ЗОТ від НСД.

Цей керівний документ встановлює класифікацію ЗОТ за рівнем захищеності від НСД до інформації на базі переліку показників захищеності та сукупності вимог, що описують їх. Під ЗОТ розуміється сукупність програмних і технічних елементів систем обробки даних, здатних функціонувати самостійно або у складі інших систем.

Ці показники містять вимоги захищеності ЗОТ від НСД до інформації та застосовуються до загальносистемних програмних засобів і операційних систем (з обліком архітектури ЕОМ). Конкретні переліки показників визначають класи захищеності ЗОТ і описуються сукупністю вимог. Сукупність усіх засобів захисту складає комплекс засобів захисту (КЗЗ).

Встановлені сім класів захищеності ЗОТ від НСД до інформації. Найнижчі вимоги пред'являються до систем, що відповідають сьомому класу, а самі високі — до першого.

Вимоги до захищеності автоматизованих систем.

Ці вимоги є складовою частиною критеріїв захищеності автоматизованих систем обробки інформації від НСД. Вимоги згруповані навколо підсистем захисту, що їх реалізовують. На відміну від інших стандартів, тут відсутній розділ що містить вимоги щодо забезпечення працездатності системи, зате є розділ, присвячений криптографічним засобам (інші стандарти не містять навіть згадки про криптографію, оскільки розглядають її виключно в якості механізму, що реалізовує інші вимоги, такі, як автентифікація, контроль цілісності і так далі). Таксономія вимог до засобів захисту АС від НСД наведена на рис 1.

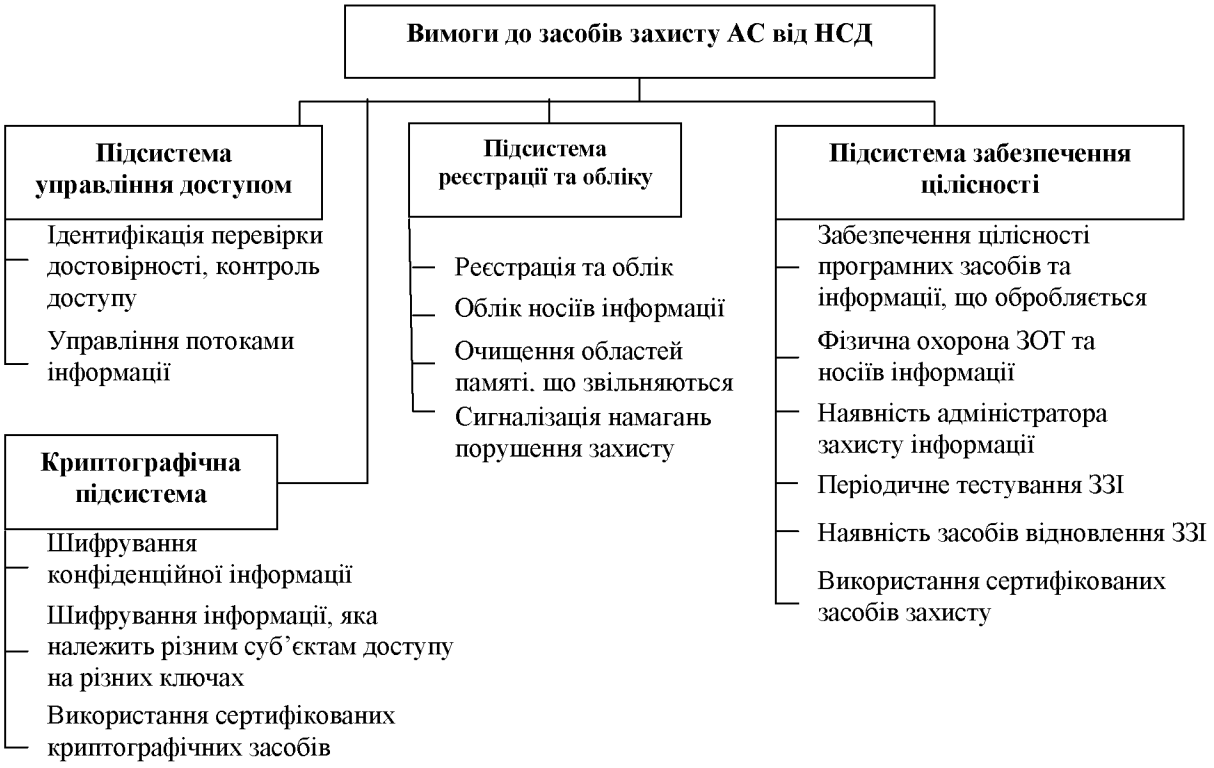

Рис. 1. Таксономія вимог до засобів захисту АС від НСД (де: ЗОТ – засоби обчислювальної техніки; ЗЗІ – засоби захисту інформації)

Класи захищеності автоматизованих систем.

Документи ДТК встановлюють дев'ять класів захищеності АС від НСД, кожен з яких характеризуються визначеною сукупністю вимог до засобів захисту. Класи підрозділяються на три групи, що відрізняються специфікою обробки інформації в АС. Група АС визначається на підставі наступних ознак:

наявність в АС інформації різного рівня конфіденційності;

рівень повноважень користувачів АС на доступ до конфіденційної інформації;

режим обробки даних в АС (колективний або індивідуальний).

В межах кожної групи дотримується ієрархія класів захищеності АС. Клас, що відповідає вищому ступеню захищеності для цієї групи, позначається індексом NA, де N - номер групи (від 1 до 3). Наступний клас позначається NБ і так далі.

Третя група включає АС, в яких працює один користувач, допущений до усієї інформації АС, яка розміщена на носіях одного рівня конфіденційності. Група містить два класи -3Б і 3А.

Друга група включає АС, в яких користувачі мають однакові повноваження доступу до усієї інформації, що обробляється і/або зберігається в АС на носіях різного рівня конфіденційності. Група містить два класи — 2Б і 2А.

Перша група включає розраховані на багато користувачів АС, в яких одночасно обробляється і/або зберігається інформація різних рівнів конфіденційності. Не всі користувачі мають рівні права доступу. Група містить п'ять класів — 1Д, 1Г. 1В, 1Б і 1А.

Висновки

Розробка керівних документів ДТК стала наслідком процесу впровадження інформаційних технологій. До початку 90-х років необхідності в подібних документах не було, оскільки у більшості випадків обробка і зберігання конфіденційної інформації здійснювалися без застосування обчислювальної техніки. Тому розробка стандартів подібного роду є абсолютно новою і невідомою областю діяльності для відповідних інститутів та установ, що дозволяє трактувати дані документи як першу стадію формування стандартів в області інформаційної безпеки.

На розробку цих документів найбільший вплив зробила "Помаранчева книга", проте вплив, в основному, відображається в орієнтуванні обох документів на системи військового застосування та у використанні єдиної універсальної шкали ступеня захищеності.

До недоліків цього стандарту відносяться відсутність вимог до захисту від загроз працездатності, орієнтація на протидію НСД та відсутність вимог до адекватності реалізації політики безпеки.

Поняття "Політика безпеки" трактується виключно як підтримка режиму секретності та відсутність НСД, що принципово невірно. Завдяки цьому засоби захисту орієнтуються виключно на протидію зовнішнім загрозам, а до структури самої системи і її функціонування не пред'являється ніяких вимог. Ранжирування вимог по класах захищеності в порівнянні з іншими стандартами інформаційної безпеки максимально спрощено та зведено до визначення наявності чи відсутності заданого набору механізмів захисту, що істотно знижує їх гнучкість вимог і можливість практичного застосування.

Незважаючи на вказані недоліки, документ ДТК заповнили правовий вакуум в області стандартів інформаційної безпеки в Російській Федерації та на певному етапі оперативно розв'язали актуальну проблему.

Література

1. Галатенко В. А. Информационная безопасность. "Открытые системы" / Галатенко В. А., NN4-6 1995 г.

Рассматривается принцип создания стандарта информационной безопасности информационно-управляющих систем на примере руководящих документов Госттехкомиссии России.

Ключевые слова: информационная безопасность, политика безопасности, доступ, стандарт, идентификация, компьютерные системы.

The article highlights the principles of creation for information security standard for control information systems with the example of the leading documents of Russians Gostehkomissii.

Key words: informative safety, policy of safety, access, standard, authentication, computer systems.