УДК 681.322

Ігор Олександрович Ляшенко

ЄВРОПЕЙСЬКІ КРИТЕРІЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Постановка проблеми та її зв'язок із важливими науковими і практичними завданнями. Формулювання мети статті

Досвід останніх збройних конфліктів підтверджує зростання ролі управління, яке буде спиратися на досягнення інтелектуальної переваги над противником. Відповідно, майбутня система управління Збройними Силами повинна бути автоматизованою, здатною здійснювати управління в реальному масштабі часу, не потребувати значних термінів на власну трансформацію та розгортання, не залежати від характеру дій угруповань військ (сил) та знаходженні на їх озброєнні різних типів та комплексів техніки та озброєння.

Реалізація цих вимог можлива лише на основі комплексної автоматизації усіх процесів управління військами (силами) та створення єдиної автоматизованої динамічної системи управління, яка б функціонувала б в масштабі реального часу. Базовою основою такої системи управління повинні стати створені та функціонуючі по мережному принципу автоматизовані системи управління різного рівня ієрархії та функціонального призначення, які повинні бути об'єднані в єдину автоматизовану систему управління Збройних Сил.

На протязі достатньо тривалого періоду в військових аналітичних виданнях підіймаються проблеми автоматизації управління військами (силами) [1-8].

Відставання у цьому питанні від провідних країн світу та невідповідність вимогам, що висуваються до сучасних Збройних Сил війнами нового покоління пояснюється цілою низкою причин, однією з яких є відсутність єдиного стандарту інформаційної безпеки.

Стандарти інформаційної безпеки покликані створити основу взаємодії між виробниками, споживачами та експертами по кваліфікації продуктів інформаційних технологій. Оскільки кожна з цих груп має свої інтереси і свої погляди на проблему інформаційної безпеки, перед стандартами інформаційної безпеки стоїть непросте завдання — примирити ці точки зору та створити ефективний механізм взаємодії усіх сторін.

Причому обмеження потреб хоч б однієї з них приведе до неможливості взаєморозуміння і взаємодії і отже, не дозволить вирішити загальне завдання — створення захищеної системи обробки інформації. Необхідність в подібних стандартах була усвідомлена вже досить давно (за мірками розвитку інформаційних технологій) і в цьому напрямку досягнутий істотний прогрес, закріплений в новому поколінні документів розробки 90-років.

Представляється доцільним проаналізувати ці документи, зіставити їх структуру, вимоги, що містяться в них, та критерії, а також оцінити ефективність їх практичного застосування на прикладі "Європейських критеріїв безпеки інформаційних технологій". Огляд стандартів будується за наступною схемою: мета розробки, основні положення, таксономія та ранжирування вимог і критеріїв.

Виклад основного матеріалу

Після виходу "Помаранчевої книги" країни Європи спільно розробили загальні "Критерії безпеки інформаційних технологій" (Information Technology Security Evaluation Criteria), далі "Європейські критерії". Цей огляд ґрунтується на версії 1.2., що опублікована в червні 1991 року від імені відповідних органів чотирьох країн: Франції Німеччини, Нідерландів і Великобританії.

"Європейські критерії" розглядають наступні завдання засобів інформаційної безпеки:

захист інформації від несанкціонованого доступу з метою забезпечення конфіденційності;

забезпечення цілісності інформації за допомогою захисту від її несанкціонованої модифікації або знищення;

забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Для того, щоб задовольнити вимогам конфіденційності, цілісності та працездатності, необхідно реалізувати відповідний набір функцій безпеки, таких, як ідентифікація та автентифікація, управління доступом, відновлення після збоїв і т. п. Щоб засоби захисту можна було визнати ефективними, потрібно мати певну міру впевненості в правильності їх вибору та надійності функціонування. Для вирішення цієї проблеми в "Європейських критеріях" вперше вводиться поняття адекватності (assurance) засобів захисту.

Адекватність включає два аспекти: ефективність, що відображає відповідність засобів безпеки вирішуваним завданням, та коректність, що характеризує процес їх розробки та функціонування. Ефективність визначається відповідністю між завданнями, поставленими перед засобами безпеки і реалізованим набором функцій захисту — їх функціональною повнотою та узгодженістю, простотою використання, а також можливими наслідками використання зловмисниками слабких місць захисту. Під коректністю розуміється правильність і надійність реалізації функцій безпеки.

Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня адекватності їх реалізації.

У "Європейських критеріях" засоби, що мають відношення до інформаційної безпеки, розглядаються на трьох рівнях деталізації. На першому рівні розглядаються цілі, які переслідують забезпечення безпеки, другий рівень містить специфікації функцій захисту, а третій — механізми, що їх реалізовують. Специфікації функцій захисту пропонується розглядати з точки зору наступних вимог:

ідентифікація і автентифікація;
управління доступом;
підзвітність;
аудит;
повторне використання об'єктів;
цілісність інформації;
надійність обслуговування;
безпека обміну даними.

Більшість з перерахованих вимог співпадають з аналогічними вимогами "Помаранчевої книги" (Trusted Computer System Evaluation Criteria). Зупинимося лише на специфічних для "Європейських критеріїв" моментах.

Вимоги безпеки обміну даними регламентують роботу засобів, що забезпечують безпеку даних, які передаються по каналам зв'язку та включають наступні розділи:

автентифікація;
управління доступом;
конфіденційність даних;
цілісність даних;
неможливість відмови від досконалих дій.

Набір функцій безпеки може специфікуватися з використанням посилань на заздалегідь визначені класи-шаблони. У "Європейських критеріях" таких класів десять. П'ять з них (F - C1, F - C2, F - B1, F - B2, F - B3) відповідають класам безпеки "Помаранчевої книги" з аналогічними позначеннями. Розглянемо детальніше інші п'ять класів, оскільки їх вимоги відображають точку зору розробників стандарту на проблему безпеки.

Клас F - IN призначений для систем з високими потребами в забезпеченні цілісності, що типово для систем управління базами даних. Його опис заснований на концепції "ролей", які відповідають видам діяльності користувачів і наданні доступу до певних об'ємів тільки за допомогою довірених процесів. Розрізняються наступні види доступу: читання, запис, додавання, видалення, створення. перейменування та виконання об'єктів.

Клас F - AV характеризується підвищеними вимогами до забезпечення працездатності.

Це істотно, наприклад, для систем управління технологічними процесами. У вимогах цього класу вказується, що система повинна відновлюватися після відмови окремого апаратного компонента таким чином, щоб усі критично важливі функції постійно залишалися доступними. У такому ж режимі повинна відбуватися і заміна компонентів системи. Незалежно від рівня завантаження повинно гарантуватися певний час реакції системи на зовнішні події.

Клас F - DI орієнтований на розподілені системи обробки інформації.

Перед початком обміну та при отриманні даних сторони повинні мати можливість провести ідентифікацію учасників взаємодії та перевірити її достовірність. Необхідно використовувати засоби контролю та виправлення помилок. Зокрема, при пересилці даних повинні виявлятися усі випадкові чи навмисні спотворення адресної чи призначеної для користувача інформації. Знання алгоритму виявлення спотворень не повинно дозволяти зловмисникові робити нелегальну модифікацію даних, які передаються. Спроби повторної передачі повинні виявлятися раніше переданих повідомлень.

Клас F - DC приділяє особливу увагу вимогам до конфіденційності інформації, що передається. Інформація по каналах зв'язку повинна передаватися в зашифрованому вигляді. Ключі шифрування мають бути захищені від несанкціонованого доступу.

Клас F - DX пред'являє підвищені вимоги як до цілісності, так і до конфіденційності інформації. Його можна розглядати як об'єднання класів F - DI і F - DC з додатковими можливостями шифрування та захисту від аналізу трафіку. Доступ має бути обмежений до раніше переданої інформації, яка, в принципі, може сприяти проведенню крипто-аналізу.

"Європейські критерії" приділяють адекватності засобів захисту значно більше уваги, ніж функціональним вимогам. Як вже говорилося, адекватність складається з двох компонентів — ефективності та коректності роботи засобів захисту. Для оцінки ступеня адекватності використовуються наступні критерії (рис. 1).

"Європейські критерії" визначають сім рівнів адекватності - від E0 до E6 (в порядку зростання).

Рівень E0 означає мінімальну адекватність (аналог рівня D "Помаранчевої книги"). При перевірці адекватності аналізується увесь життєвий цикл системи від початкової фази проектування до експлуатації та супроводу. Рівні адекватності від E1 до E6 побудовані по наростанню вимог ретельності контролю. Так, на рівні E1 аналізується лише загальна архітектура системи, а адекватність засобів захисту підтверджується функціональним тестуванням. На рівні E3 до аналізу притягуються початкові тексти

Рис. 1. Таксономія критеріїв адекватності "Європейських критеріїв"

програм і схеми апаратного забезпечення. На рівні Е6 потрібен формальний опис функцій безпеки, загальної архітектури, а також політики безпеки.

Ступінь безпеки системи визначається найслабкішим з критично важливих механізмів захисту. У "Європейських критеріях" визначені три рівні безпеки — базовий, середній та високий. Безпека вважається базовою, якщо засоби захисту здатні протистояти окремим випадковим атакам.

Безпека вважається середньою, якщо засоби захисту здатні протистояти зловмисникам, які мають обмежені ресурси та можливості.

Нарешті, безпеку можна вважати високою, якщо є впевненість, що засоби захисту можуть бути здолані тільки зловмисником з високою кваліфікацією, набір можливостей і ресурсів якого виходить за рамки розумного.

Висновки

"Європейські критерії безпеки інформаційних технологій", що з'явилися за "Помаранчевою книгою", зробили істотний вплив на стандарти безпеки та методику сертифікації. Головне досягнення цього документа — введення поняття адекватності засобів захисту та визначення окремої шкали для критеріїв адекватності. Як вже згадувалося. "Європейські критерії" надають адекватності засобів захисту навіть більше значення, ніж їх функціональності. Цей підхід використовується у багатьох стандартах інформаційної безпеки, які з'явилися пізніше.

Необхідно відмітити, що "Європейські критерії" тісно пов'язані з "Помаранчевою книгою", що робить їх не зовсім самостійним документом. На перший погляд досить дивним виглядає той факт, що "Європейські критерії" визнають можливість наявності недоліків в сертифікованих системах (критерій можливості використання недоліків захисту), проте насправді це свідчить про тверезий погляд на існуюче положення та визнання того очевидного факту, що реальні системи ще дуже недосконалі і далекі від ідеалу.

Література

1. Петряков Ю. Еще раз об АСУ с опорой на собственные силы // Петряков Ю. // Независимое военное обозрение. – 14.05.2004. **2. Синявский В.** Возможные подходы к созданию автоматизированных систем управления войсками (силами) // В.К. Синявский // Наука и военная безопасность. – 2008. №3. – С.21-27. **3. Литошенко А.** АСУ: выбор вектора развития. Будущее – за глобальным информационным полем // Литошенко А. // Воздушно-космическая оборона. – 2007. – №6(37). – С.38-45. **4. Системы** и средства управления вооруженных сил ведущих зарубежных стран и направления их развития (информационно-аналитический обзор). – Мн. ГУ "НИИ ВС РБ". – 2007. – 303 с. **5. Куликов А.** Война в едином информационном пространстве // Куликов А. // Воздушно-космическая оборона. – 2008. – № 2. – С.54-60. **6. Барвиненко В.** Об автоматизации управления группировками Вооруженных Сил // Барвиненко В.В. // Военная мысль. – 2008. - № 8. – С. 9-16. **7. Вервейко Б.** Особенности моделирования системы управления Вооруженных Сил как сложной организационно-технической системы // Б.М. Вервейко, С.К. Гульбис // Наука и военная безопасность. – 2010. №1. – С.26-29. **8. Косс В.А.** Особливості процедур планового й кризового управління військовими формуваннями.// Наука і оборона №1-2004р. - С.25-32

Рассматривается принцип создания стандарта информационной безопасности информационно-управляющих систем на примере "Европейских критериев информационной безопасности".

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

The article highlights the principles of creation for information security standard for control information systems with the example of the "European criteria of information safety".

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