1. Дослідження існуючих стандартів шодо побудови систем захисту інформації
   1. Основні стандарти в сфері забезпечення інформаційної безпеки

Будь-яке забезпечення інформаційної безпеки потребує контролю і перевірки, яка не може бути проведена тільки методом індивідуальної оцінки, без урахування міжнародних і державних стандартів.

Формування стандартів інформаційної безпеки відбувається після чіткого визначення її функцій і меж. Інформаційна безпека - це забезпечення конфіденційності, цілісності та доступності даних.

Для визначення стану інформаційної безпеки найбільш застосовна якісна оцінка, так як висловити ступінь захищеності або уразливості в процентному співвідношенні можливо, але це не дає повної і об'єктивної картини.

Для оцінки і аудиту безпеки інформаційних систем можна застосувати ряд інструкції і рекомендацій, які і мають на увазі під собою нормативне забезпечення.

Контроль і оцінка стану безпеки здійснюється шляхом перевірки їх відповідності стандартам державним (ГОСТ, ІСО) і міжнародним (Iso, Common criteris for IT security).

Міжнародний комплекс стандартів, розроблених Міжнародною Організацією по Стандартизації (ISO), являє собою сукупність практик і рекомендацій щодо впровадження систем і устаткування інформаційної захисту.

Найвідоміші стандарти в сфері забезпечення інформаційної безпеки наведено нижче

* Критерій оцінки надійності комп'ютерних систем «Помаранчева книга» (США);
* Гармонізовані критерії європейських країн;
* Рекомендації Х.800;
* Cтандарт BSI;
* Стандарт BS 7799;
* Стандарт «Загальні критерії» ISO 15408;
* Стандарт ISO 17799;
* Стандарт COBIT
* Система стандартів NIST
* Стандарти НД ТЗІ
  1. Огляд системи стандартів NIST

**Націона́льний інститу́т станда́́ртів і техноло́гії** (NIST, до 1988 відомий як **Національне бюро стандартів**)— національний орган зі [стандартизації](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F) у [США](https://uk.wikipedia.org/wiki/%D0%A1%D0%A8%D0%90).

NIST — неурядова некомерційна організація, що координує роботи з добровільної [стандартизації](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F) в приватному секторі економіки, керує діяльністю організацій-розробників [стандартів](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) і приймає рішення про надання стандарту статусу національного (якщо в ньому зацікавлені різні фірми і стандарт набуває міжгалузевого характеру).

NIST є єдиною організацією в США, що приймає (затверджує) національні (федеральні) стандарти. Це відповідає основному завданню NIST — сприяння вирішенню проблем, що мають загальнодержавне значення (економія енергоресурсів, захист навколишнього середовища, забезпечення безпеки життя людей і умов виробництва).

Інститут розробляє цільові програми. Програмно-цільове планування охоплює виробництво і транспортування палива, постачання електроенергією, застосування ядерної, сонячної та інших видів енергії. Значно менше уваги приділяється розробці стандартів на готову продукцію, оскільки в цій області діють фірмові нормативні документи.

Спеціальна публікація NIST 800-53 - це частина спеціальної публікації 800-серії, яка звітує про дослідження, керівні принципи та інформаційну діяльність лабораторії інформаційних технологій (ITL) в галузі безпеки інформаційної системи та про діяльність ITL з промисловістю, урядом та академічними організаціями.

Зокрема, NIST Special Publication 800-53 охоплює кроки в рамках управління ризиками, які стосуються вибору контролю безпеки для федеральних інформаційних систем відповідно до вимог безпеки в Федеральному стандарті обробки інформації (FIPS) 200. Це включає в себе вибір початкового набору базової безпеки контроль на основі аналізу найгіршого впливу FIPS 199, розробка базового контролю безпеки та доповнення контролю безпеки на основі організаційної оцінки ризику. Правила безпеки охоплюють 17 областей, включаючи контроль доступу, реакцію на інциденти, безперервність бізнесу та відновлення можливостей після аварій.

Ключовою частиною процесу сертифікації та акредитації для федеральних інформаційних систем є відбір та реалізація підмножини контролю (гарантій) з каталогу контролю безпеки (NIST 800-53, додаток F). Ці засоби контролю - це управління, оперативні та технічні гарантії (або контрзаходи), встановлені для інформаційної системи для захисту конфіденційності, цілісності та наявності системи та її інформації. Для здійснення необхідних гарантій або контролю агентства повинні спочатку визначити категорію безпеки своїх інформаційних систем відповідно до положень FIPS 199 "Стандарти для категоризації безпеки Федеральних інформаційно-інформаційних систем". Класифікація безпеки інформаційної системи (низька , середній або високий) визначає базовий набір елементів керування, які повинні бути впроваджені та контрольовані. Агентства мають можливість регулювати ці елементи керування та адаптувати їх до більш точної відповідності їхніх організаційних цілей або середовищам.

Даний стандарт описує контролі безпеки, а також інструкції про те, як ними правильно користуватись. Всі контролі в стандарті розбиті на сім'ї, що відповідають різним областям забезпечення інформаційної безпеки. Сімейства контролів, якими оперує NIST наведено в таблиці 1.

Таблиця 1.

|  |  |  |
| --- | --- | --- |
| Скорочення | Сімейство контролю (оригінальна назва) | Переклад |
| AT | Awareness and Training | Обізнаність та навчання |
| AU | Audit and Accountability | Аудит та звітність |
| CA | Security Assessment and Authorization | Авторизація та оцінка безпеки |
| CM | Configuration Management | Керування конфігурацією |
| CP | Contingency Planning | Планування безперервності бізнесу |
| IA | Identification and Authentication | Ідентифікація та автентифікація |
| IR | Incident Response | Реагування на інциденти |
| MA | Maintenance | Підтримка |
| MP | Media Protection | Захист носіїв інформації |
| PE | Physical and Environmental Protection | Захист від впливу середовища |
| PL | Planning | Планування |
| PS | Personnel Security | Безпека персоналу |
| RA | Risk Assessment | Оцінка ризиків |
| SA | System and Services Acquisition | Придбання систем та сервісів |
| SC | System and Communications Protection | Захист систем та комунікацій |
| SI | System and Information Integrity | Цілісність систем та інформації |
| PM | Program Management | Керування програмою ІБ |

Опис контролю відповідає певному шаблону. Перш за все вказано код сімейства контролю і номер, наприклад, AU-3. Далі вказано назву контролю безпеки.

Після цього йдуть наступні розділи:

* Control. Опис особливих дій або активностей, що відносяться до безпеки, які виконуються в організації або ІС. Для деяких контролів передбачені можливості гнучкого налаштування, надаючи можливість організації визначати деякі параметри, пов'язані з контролем. Наприклад, таким параметром може бути частота проведення аудиту, термін зберігання логів або кількість невдалих спроб авторизації користувача. Таким чином можна підганяти контроль під конкретні потреби, грунтуючись на вимогах, пропонованих до безпеки з боку бізнес цілей організації, результати оцінки ризиків та прийнятності ризиків, а також вимоги законів і регуляторів.
* Supplemental Guidance. Додаткова інформація для конкретного контролю. Може включати пояснювальну інформацію щодо реалізації або використання контролю і т.д. Також можуть зазначатися посилання на інші пов'язані контролі.
* Control Enhancements. У даній секції представлені можливості для «поліпшення» контролю, шляхом додавання до нього додаткової функціональності або його посилення.
* References. Тут зібрані посилання на закони, нормативні акти, стандарти, вимоги регуляторів, різні керівництва і т.д.
* Priority and Baseline Allocation. Має вигляд таблички, в якій представлено інформацію щодо рекоменддованого пріоритету в процесі прийняття рішення про реалізацію контролів, а також початковий розподіл контролю по базовим наборах для систем з різним рівнем критичності. Пріоритет впровадження дозволяє організації здійснювати реалізацію контролів в більш ефективній і своєчасній послідовності, в першу чергу впроваджуючи основоположні заходи.

Для упорядкування та забезпечення структурного підходу передбачено поділ контролів на різні типи, в залежності від їх призначення:

* Common. Основні контролі, які можуть успадковуватися різними системами і мають вплив поза масштабів окремо взятої ІС. Система успадковує контроль безпеки в разі, якщо він здійснює свою функцію безпеки в цій ІС, проте був розроблений, реалізований, оцінений, авторизований поза цією ІС
* System-specific. Контроль знаходиться в зоні відповідальності власників конкретної ІС.
* Hybrid. Частина контролю функціонує в якості загального, а частина в якості системного контролю.

* 1. Критерій оцінки надійності комп'ютерних систем «Помаранчева книга» (США)

Офіційною назвою данного стандарту є «Критерії визначення безпеки комп'ютерних систем»

Критерії визначення безпеки комп'ютерних систем (англ. Trusted Computer System Evaluation Criteria) - стандарт Міністерства оборони США, який встановлює основні умови для оцінки ефективності засобів комп'ютерної безпеки, що містяться в комп'ютерній системі. Критерії використовуються для визначення, класифікації та вибору комп'ютерних систем, призначених для обробки, зберігання та пошуку важливої або секретної інформації.

При розробці критеріїв переслідувались три мети:

* запропонувати користувачам критерій, за допомогою якого можна було б оцінювати ступінь довіри до обчислювальної системи з точки зору забезпечення безпеки обробки секретної та іншої критично важливої інформації;
* створити керівництво, покликане допомогти виробникам вибрати з широкого діапазону пристроїв ті, які доцільно вбудовувати в їх нові, широко представлені на ринку перевірені комерційні продукти;
* забезпечити основу для оцінки вимог до захищеності в специфікаціях придбаних продуктів

"Помаранчева книга" пояснює поняття безпечної системи, як таку, що "керує, за допомогою відповідних засобів, доступом до інформації, так що тільки належним чином авторизовані особи або процеси, що діють від їх імені, отримують право читати, записувати, створювати і видаляти інформацію".

В "Помаранчевій книзі" довірена система визначається як "система, яка використовує достатні апаратні і програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу". ІС розбивають на чотири широких ієрархічних класи підвищеного забезпечення секретності. Вони є основою для оцінки ефективності засобів управління захистом, вбудованих в продукти типу автоматизованих систем обробки даних.

У розглянутих Критеріях і безпеку, і довіру оцінюються виключно з точки зору управління доступом до даних, що є одним із засобів забезпечення конфіденційності і цілісності (статичної). Питання доступності в "Помаранчевій книзі" не розглядаються.

Основними критеріями для оцінки ступеню довіри є:

* Політика безпеки - набір законів, правил і норм поведінки, що визначають, як організація обробляє, захищає і поширює інформацію. Зокрема, правила визначають, в яких випадках користувач може оперувати конкретними наборами даних. Чим вище ступінь довіри системі, тим суворіше і різноманітніше повинна бути політика безпеки. Залежно від сформульованої політики можна вибирати конкретні механізми забезпечення безпеки. Політика безпеки - це активний аспект захисту, що включає в себе аналіз можливих загроз і вибір заходів протидії.
* Рівень гарантованості - міра довіри, яка може бути надана архітектурі і реалізації ІС. Довіра безпеки може виникати як з аналізу результатів тестування, так і з перевірки (формальної чи ні) загального задуму і реалізації системи в цілому і окремих її компонентів. Рівень гарантованості показує, наскільки коректні механізми, що відповідають за реалізацію політики безпеки. Це пасивний аспект захисту.

Вимоги, що пред'являються до комп'ютерної системи (продукту) в процесі оцінювання, умовно можна розділити на чотири типи - вимоги проведення послідовної політики безпеки (security policy), вимоги ведення обліку використання продукту (accounts), вимоги довіри до продукту (assurance) і вимоги до документації на продукт.

Згідно TCSEC, для оцінювання комп'ютерних систем виділено чотири основних групи безпеки, які в свою чергу діляться на класи безпеки:

* группа Д - Minimal Protection (минимальная защита) - объединяет компьютерные системы, не удовлетворяющие требованиям безопасности высших классов. В данном случае группа и класс совпадают;
* група С - Discretionary Protection (виборча захист) - об'єднує системи, що забезпечують набір засобів захисту, що застосовуються користувачем, включаючи засоби загального контролю і обліку суб'єктів та їх дій. Ця група має два класи:
  + клас С1 - Discretionary Security Protection (виборча захист безпеки) - об'єднує системи з поділом користувачів і даних;
  + клас С2 - Controlled Access Protection (захист контрольованого доступу) - об'єднує системи, що забезпечують більш тонкі засоби захисту в порівнянні з системами класу С1, що роблять користувачів індивідуально помітними в їх діях за допомогою процедур контролю входу та контролю за подіями, що зачіпають безпеку системи і ізоляцію даних.
* група В - Mandatory Protection (обов’язковий захист) - має три класи:
  + клас В1 - Labeled Security Protection (захист безпеки з використанням міток) - об'єднує системи, що задовольняють всім вимогам класу С2, додатково реалізуючу заздалегідь визначену модель безпеки, що підтримують мітки суб'єктів і об'єктів, повний контроль доступу. Вся видана інформація реєструється, всі виявлені при тестуванні недоліки повинні бути усунені;
  + клас В2 - Structured Protection (структурована захист) - об'єднує системи, в яких реалізована чітко визначена і задокументована формалізована модель забезпечення безпеки, а меточного механізм поділу і контролю доступу, реалізований в системах класу В1, поширений на всіх користувачів, всі дані і всі види доступу . У порівнянні з класом В1 посилені вимоги щодо ідентифікації користувачів, контролю за виконанням команд керування, посилена підтримка адміністратора і операторів системи. Повинні бути проаналізовані і перекриті всі можливості обходу захисту. Системи класу В2 вважаються "відносно невразливими" для несанкціонованого доступу;
  + клас В3 - Security Domains (області безпеки) - об'єднує системи, що мають спеціальні комплекси безпеки. У системах цього класу повинен бути механізм реєстрації всіх видів доступу будь-якого суб'єкта до будь-якого об'єкту. Повинна бути повністю виключена можливість несанкціонованого доступу. Система безпеки повинна мати невеликий обсяг і прийнятну складність для того, щоб користувач міг у будь-який момент протестувати механізм безпеки. Системи цього класу повинні мати засоби підтримки адміністратора безпеки; механізм контролю повинен бути поширений аж до сигналізації про всі події, які зачіпають безпеку; повинні бути кошти відновлення системи. Системи цього класу вважаються стійкими до несанкціонованого доступу.
* група А - Verified Protection (захист перевіряється) - об'єднує системи, характерні тим, що для перевірки реалізованих в системі засобів захисту оброблюваної або інформації, що зберігається застосовуються формальні методи. Обов'язковою вимогою є повне документування всіх аспектів проектування, розробки і виконання систем. Виділено єдиний клас:
  + клас А1 - Verified Desing (перевіряється розробка) - об'єднує системи, функціонально еквівалентні системам класу В3 і не потребують будь-яких додаткових коштів. Відмінною рисою систем цього класу є аналіз формальних специфікацій проекту системи і технології виконання, що дає в результаті високу ступінь гарантованості коректного виконання системи. Крім цього, системи повинні мати потужні засоби управління конфігурацією і засоби підтримки адміністратора безпеки.
  1. Common Criteria

Common Criteria є основою, в якій користувачі комп'ютерної системи можуть визначати свої функціональні вимоги щодо безпеки та вимоги забезпечення (відповідно SFRs та SARs) у цільовому забезпеченні безпеки (ST) і можуть бути взяті з профілів захисту (PP). Постачальники можуть потім реалізувати або подавати заяви про атрибути безпеки своєї продукції, а тестові лабораторії можуть оцінити продукти, щоб визначити, чи дійсно вони відповідають вимогам. Іншими словами, Загальні критерії забезпечують впевненість, що процес специфікації, впровадження та оцінки продукту комп'ютерної безпеки був проведений строго, стандартно та повторюваним чином на рівні, який відповідає цільовій середовищі для використання

Основними відмітними рисами Загальних критеріїв є:

* Найбільш повна на сьогоднішній день сукупність вимог безпеки інформаційних технологій.
* Чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. Функціональні вимоги відносяться до функцій безпеки (ідентифікація, аутентифікація, управління доступом, аудит і т.д.), а вимоги довіри - до технології розробки, тестування, аналізу вразливостей, постачання, супроводу, експлуатаційної документації, тобто до всіх етапів життєвого циклу виробів інформаційні технології.
* Систематизація і класифікація вимог по ієрархії "клас" - "сімейство" - "компонент" - "елемент" з унікальними ідентифікаторами вимог, що забезпечує зручність використання.
* Ранжування компонентів вимог в родинах і класах за ступенем повноти і жорсткості, а також їх групування в пакети функціональних вимог і оціночні рівні довіри.
* Гнучкість і динамізм в підході до завдання вимог безпеки для різних типів виробів інформаційних технологій і умов їх застосування, що забезпечуються шляхом цілеспрямованого формування необхідних наборів вимог у вигляді визначених у ЗК стандартизованих структур (профілів захисту і завдань з безпеки).
* Відкритість для подальшого нарощування сукупності вимог.

Предметом розгляду в ЗК є програмно-технічні та технологічні заходи забезпечення безпеки ІТ. До аспектів забезпечення безпеки ІТ, які знаходяться поза рамками ЗК, відносяться:

* адміністративні (організаційні) заходи забезпечення безпеки, не пов'язані безпосередньо із забезпеченням безпеки ІТ. Адміністративні заходи розглядаються в тій мірі, в якій вони здатні вплинути на можливості функцій безпеки протистояти загрозам безпеки ІТ;
* оцінка технічних аспектів забезпечення безпеки (таких, як захист від витоку інформації технічними каналами, що виникають за рахунок побічного електромагнітного випромінювання і наведень). Разом з тим, багато положень ЗК застосовні і в цій області;
* методологія оцінки, адміністративна та правова система застосування критеріїв оцінки органами, що здійснюють оцінку. Однак очікується, що ОК будуть використовуватися для цілей оцінки в контексті такої системи і такої методології;
* процедури використання результатів оцінки при атестації виробів ІТ;

Серед користувачів ОК можна виділити наступні групи :

* системні фахівці, що відповідають за визначення і виконання політики і вимог безпеки організації в області ІТ;
* аудитори, які контролюють адекватність заходів безпеки системи;
* проектувальники систем безпеки, що визначають специфікацію функцій безпеки виробів ІТ;
* особи, які здійснюють атестацію систем ІТ в конкретному середовищі функціонування;
* замовники виробів ІТ, що визначають вимоги до оцінки і підтримують її проведення;
* органи сертифікації, що здійснюють керівництво і нагляд за програмами проведення оцінок.

Як показують оцінки фахівців в області інформаційної безпеки, за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ЗК представляють найбільш досконалий з існуючих в цій галузі стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку і являє собою базовий стандарт, що містить методологію завдання вимог безпеки ІТ, а також систематизований каталог вимог безпеки. В якості функціональних стандартів, в яких формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені і будь-які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

* 1. Рекомендації Х.800

Рекомендації х.800 визначає сервіси, характерні для розподілених систем, рівня семирівневої моделі, на якій можуть бути реалізовані механізми безпеки, функції безпеки, а також адміністрування засобів безпеки.

Виділяють наступні сервіси безпеки і виконувані ними ролі:

Аутентифікація. Даний сервіс забезпечує перевірку автентичності партнерів по спілкуванню і перевірку автентичності джерела даних. Аутентифікація партнерів по спілкуванню використовується при встановленні з'єднання і, можливо, періодично під час сеансу. Вона служить для запобігання таких загроз, як маскарад і повтор попереднього сеансу зв'язку. Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність серверу) і двосторонньої (взаємної).

Управління доступом. Забезпечує захист від несанкціонованого використання ресурсів, доступних через мережу.

Політика приватності. Забезпечує захист від несанкціонованого отримання інформації. Окремо згадаємо конфіденційність трафіку (це захист інформації, яку можна отримати, аналізуючи мережеві потоки даних).

Цілісність даних поділяється на підвиди залежно від того, який тип спілкування використовують партнери - з встановленням з'єднання або без нього, захищаються чи всі дані або тільки окремі поля, чи забезпечується відновлення в разі порушення цілісності.

Невідмовності (неможливість відмовитися від вчинених дій) забезпечує два види послуг: неспростовності з підтвердженням справжності джерела даних і неспростовності з підтвердженням доставки. Побічним продуктом неспростовності є аутентифікація джерела даних.

# Німецький стандарт BSI

В 1998 році в Німеччині було опубліковано "Керівництво по захисту інформаційних технологій для базового рівня". Пізніше його було представлено як стандарт BSI. В основу покладена загальна методологія і компоненти управління інформаційною безпекою, які наведено нижче:

* Загальний спосіб управління безпекою інформації (організація системи менеджменту у сфері інформаційної безпеки, методи використання керівництва)
* Опис компонентів ІТ
* Найважливіші компоненти (організаційний та процедурний рівні, організація захисту інформації, планування дій в надзвичайних ситуаціях)
* Інфраструктура
* Різнотипні клієнтські компоненти (такі як: DOS, Windows, UNIX, мобільні компоненти та інші)
* Різні типи Мережі (з'єднання «точка-точка», мережі по типу Novell NetWare, мережі, що використовують OC ONIX і Windows, різнорідні мережі)
* Різні елементи систем передачі даних (такі як електронна пошта, модеми, міжмережеві екрани та інше).
* Телекомунікаційні системи
* Стандартне ПО
* Бази даних
* Визначення основних компонентів налагодження режиму інформаційної безпеки (організаційний і технічний рівні захисту даних, планування дій в надзвичайних ситуаціях, підтримка безперервності бізнесу).
* Характеристики об'єктів, які підлягають інформатизації
* Опис доступних інформаційних активів певної компанії(до активів відносять, наприклад, апаратне і програмне забезпечення, таке як комп’ютери та сервери під керуванням ОС DOS, Windows або UNIX)
* Характеристики мереж комп’ютерів заснованих на різних технологіях
* Технічні характеристики ТК обладнання, як активного, так і пасивного
* Вичерпні каталоги з загрозами безпеці та заходами контролю (в кожному визначено більше за 600 найменувань)

Cтандарт BSI поділив усі загрози на класи, наведені нижче:

* Форс-мажорні та надзвичайні обставини
* Нестача заходів, пов’язаних з організацією
* Людський фактор
* Технічні несправності
* Дії, вчинені навмисно

Схожим чином прокласифіковано заходи протидії:

* Покращення інфраструктури
* Адміністративні контрзаходи
* Процедурні контрзаходи
* Програмно-технічні контрзаходи
* Зниження вразливості комунікацій; розробка плану дій в надзвичайних ситуаціях
  1. COBIT

Управління ІТ - складова частина успіху в управлінні підприємством, яка гарантує раціональне і ефективне вдосконалення всіх взаємопов'язаних процесів підприємства. Управління ІТ надає основу, яка пов'язує ІТ-процеси, ІТ-ресурси і інформацію зі стратегією і цілями організації, що дозволяє максимально ефективно використовувати інформацію, підвищуючи капіталізацію і отримуючи конкурентоспроможні переваги.

Принципи управління створені для того, щоб допомогти керівнику ІТ відповісти на три стратегічних питання:

1. Чи існують зараз у організації Інформаційні технології, при керуванні якими "задовольняються" всі інформаційні потреби організації?
2. Як організація забезпечує інфраструктуру та управляє ризиками, наскільки організація залежить від цього?
3. З якими проблемами організація стикається при управлінні ІТ?

Щоб отримати відповіді на ці стратегічні питання необхідно безперервно відповідати на "тактичні" питання:

* Що є результатом ІТ-процесів?
* Що є рішенням проблем в ІТ?
* З чого складаються ці рішення?
* Чи будуть працювати ці рішення?
* Як їх реалізувати?

Для отримання відповідей на "тактичні" питання в книзі Принципи управління CobiT, включені Моделі Зрілості, Критичні Фактори Успіху (КФУ), Ключові Індикатори Цілі (КІЦ) і Ключові Показники Результату (КПР), це доповнення дало змогу отримати якісно покращений підхід до питань управління ІТ , який відповідає потребам керівників в частині управління і контролю.

Моделі зрілості в CobiT призначені для контролю над ІТ-процесами організації. Вони базуються на визначенні рівня розвитку організації від неіснуючого до оптимізованого (від 0 до 5 рівня моделі зрілості). Цей підхід був привнесений в CobiT з Моделей Зрілості, розроблених Інститутом проектування і розробки програмного забезпечення (Software Engineering Institute), створених для оцінки рівня зрілості розробки програмного забезпечення.

Моделі зрілості НЕ підказують як поліпшити роботу компанії і не пояснюють, як працювати з персоналом, також немає готових посібників і по застосуванню моделей зрілості. Рекомендується кожної конкретної компанії розробити подібне керівництво для свого бізнесу або запросити сторонніх консультантів для вирішення цього питання. Моделі зрілості призначені для організації ефективного управління. Вони визначають ключові дії, які вказують, що треба зробити для досягнення необхідної якості і містять способи контролю над правильністю виконання ключових ІТ-процесів і методи їх коригування. Ключові дії детально описані в Керівництві на абстрактному рівні, а в процесі використання MM компанія може вибрати довільну ступінь їх формалізації.

Шкала моделей зрілості:

* 0. Не існує. Повна відсутність будь-яких процесів управління ІТ. Організація не визнає існування проблем в ІТ, які потрібно вирішувати, і, таким чином, немає ніяких відомостей про проблеми.
* 1. Початок (Анархія). Організація визнає існування проблем управління ІТ та необхідність їх вирішення. При цьому не існує ніяких стандартизованих рішень. Існують випадкові одномоментні рішення, що приймаються кимось персонально або від випадку до випадку. Підхід керівництва до вирішення ІТ-проблем хаотичний, визнання існування проблем випадково і непослідовно.
* 2. Повторення (Фольклор). Існує загальне усвідомлення проблем управління ІТ. Показники діяльності та ІТ-процесів знаходяться в розвитку, охоплюючи процеси планування, функціонування та моніторингу ІТ. Діяльність з управління інформаційними технологіями описана і інтегрована в процес управління організацією. Обрані для поліпшення і / або контролю ті ІТ-процеси, які впливають на основні бізнес-процеси підприємства. Ефективно здійснюється планування і управління інвестиціями. Керівництво організації регламентувало заходи з управління ІТ, а також методи управління і оцінки, але процес не був прийнятий в організації. Не існує формалізованого навчання, набору взаємопов'язаних стандартних процедур управління, відповідальність покладена на співробітників. Співробітники контролюють процеси управління за допомогою проектів та ІТ-процесів. Обмежені інструменти управління вибираються і впроваджуються для збору метрик управління, але не використовуються в повному обсязі через недоліки в оцінці їх функціональності.
* 3. Опис (Стандарти). Необхідність діяти відповідно до принципів управління ІТ розуміється і приймається. Розвивається базовий набір показників управління ІТ: визначено зв'язок між результатом і показниками продуктивності, вона зафіксована і впроваджена в стратегічні процеси планування і моніторингу. Процедури стандартизовані і задокументовані, проводиться навчання співробітників по виконанню цих процедур. Показники продуктивності всіх видів діяльності зафіксовані і відслідковуються, що призводить до підвищення ефективності роботи всієї організації. Процедури не складні, вони є формалізацією існуючої практики. Ідеї ​​збалансованих карт оцінки бізнесу приймаються організацією. Відповідальність за навчання, виконання та застосування стандартів покладено на співробітників організації. Аналіз першопричин застосовується час-від-часу. Більшість процесів працюють відповідно до деякими основними метриками, і, як правило, окремими співробітниками, тому ні про які відхиленнях керівники не знають. Однак загальна звітність про виконання ключових процесів є чіткою, і керівництво преміює співробітників на основі вимірювання ключових результатів.
* 4. Управління (Вимірюваний). Існує повне розуміння проблем управління ІТ на всіх рівнях організації, постійно відбувається навчання співробітників. Визначено і підтримуються в актуальному стані угоди про рівень обслуговування. Чітко розподілена відповідальність, встановлений рівень володіння процесами. Процеси ІТ відповідають бізнесу і стратегії ІТ. В першу чергу поліпшення в процесах ІТ грунтуються на вимірюваних кількісних показниках. Існує можливість управляти процедурами і метриками процесів, вимірювати їх відповідність. Всі співвласники процесу усвідомлюють ризики, важливість ІТ і можливості, які вони надають. Керівництво організації визначило допустимі відхилення, при яких процеси повинні працювати. Якщо процеси не працюють ефективно і продуктивно, дії робляться в багатьох (але не всіх випадках). Процеси постійно вдосконалюються, їх результати відповідають "найкращих практик". Формалізований порядок аналізу першопричин. Присутній розуміння необхідності постійного вдосконалення. Обмежено застосовуються передові технології, засновані на сучасній інфраструктурі і модифікованих стандартних інструментах. Всі необхідні ІТ-фахівці залучені в бізнес-процеси. Управління ІТ перетворюється в процес рівня всієї організації. Діяльність управління ІТ інтегрується в процес управління організацією.
* 5. Оптимізація. В організації існує поглиблене розуміння управління ІТ, проблем і рішень ІТ, а також перспектив. Навчання і комунікація підтримуються на належному рівні, найсучаснішими засобами. В результаті безперервного поліпшення процеси відповідають моделям зрілості, побудованим на підставі "кращої практики". Впровадження цих процедур призвело до появи організацій, людей і процесів, максимально адаптуються до умов, що змінюються, а також повністю відповідають вимогам управління ІТ. Першопричини всіх проблем і відхилень ретельно аналізуються, за результатами аналізу виконуються результативні дії. Інформаційні технології інтегровані в бізнес-процеси, повністю їх автоматизують, надаючи можливість підвищувати якість і ефективність роботи організації.

Критичні Фактори Успіху (КФУ)

Критичні Фактори Успіху (КФУ) - визначають найбільш важливі проблеми або дії керівників, спрямовані на досягнення контролю над ІТ-процесами. КФУ повинні бути керованими, орієнтованими на успіх і описувати, як виконувати необхідні стратегічні, технічні, організаційні або процедурні дії для досягнення успіху.

Приклади Критичних Факторів Успіху (КФУ):

* Дії з управління ІТ інтегровані в процеси управління організації і стиль роботи керівників;
* Управління ІТ зосереджено на цілях організації: стратегічні ініціативи, використанні технологій для розвитку бізнесу, достатності ресурсів і задоволення бізнес-вимог;
* Дії з управління ІТ ясно визначені, формалізовані і здійснюються на основі потреб підприємства з відповідною звітністю;
* Методи управління розроблені для збільшення продуктивності, оптимального використання ресурсів і збільшення ефективності ІТ-процесів;
* Організаційні методи стежать за навколишнім середовищем і культурою управління; сприяють нормальному контролю; ведення стандартної практики управління ризиками; визначають ступінь відповідності встановленим стандартам; керують і вивчають недоліки і ризики;
* Методи аудиту визначені таким чином, щоб уникнути збоїв і помилок в системі внутрішнього контролю;
* Спостерігається інтеграція і розвиток взаємодії складних ІТ-процесів, таких як управління проблемами, змінами та конфігураціями;
* Засновано контрольний комітет, який призначає і спостерігає за незалежним аудитом, який приділяє пильну увагу ІТ при складанні планів аудиту, а також приймає до уваги результати досліджень сторонніх організацій і аудіторов

Ключові Індикатори Цілі (КІЦ)

Ключові Індикатори Цілі (КІЦ) описують комплекс вимірювань, які за фактом повідомляють керівництву, що ІТ-процес досяг пропонованих бізнес-вимог. КІЦ виражається в термінах інформаційних критеріїв:

* Придатність інформації, необхідної для підтримки бізнесу;
* Ризики відсутності цілісності і конфіденційності;
* Рентабельність процесів і операцій;
* Підтвердження надійності, ефективності та узгодженості.

Ключові Індикатори Результату (КІР)

Ключові Індикатори Результату (КИР) описують комплекс дій, необхідних для визначення, наскільки ІТ-процеси досягають поставлених цілей. КИР є основними індикаторами, що відображають ймовірність досягнення мети. А також індикаторами, що вказують адекватність способів, методів і навичок, що використовуються при досягненні результату.

Ключовими Індикаторами Результату (КИР), можуть бути:

* Збільшення рентабельності ІТ-процесів;
* Поліпшення роботи і планування дій щодо вдосконалення ІТ-процесів;
* Збільшення навантаження на ІТ-інфраструктуру;
* Підвищення ступеня задоволення користувачів (опитування користувачів і кількість скарг);
* Поліпшення взаємодії і комунікацій між керівниками ІТ і керівництвом організації
* Підвищення продуктивності співробітників.

Управління ІТ по CobiT

Потреби бізнесу визначаються Ключовими Індикаторами Цілі, чому сприяє організація постійного контролю над усіма ресурсами ІТ. Досягнення необхідного рівня контролю вимірюється Ключовими Показниками Результату, які враховують Критичні Фактори Успіху.

Модель Зрілості використовується для оцінки рівня управління ІТ в даній організації - від неіснуючого (найнижчий рівень) до оптимізованого (найвищий рівень).

Для досягнення п'ятого, "оптимізованого" рівня зрілості в управлінні ІТ організація повинна бути, принаймні, на п'ятому рівні в домені моніторинг і як мінімум на четвертому рівні моделей зрілості для всіх інших доменів.

* 1. Стандарти НД ТЗІ
     1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»

Даний стандарт дає наступне визначення інформаційно-телекомунікаційній системі. Це така система, що належить до одного з видів автоматизованих систем: інформаційна система, телекомунікаційна система, інтегрована система.

Інформаційна система – організаційно-технічна система, яка реалізує технологію обробки інформації з використанням засобів обчислювальної техніки та програмного забезпечення;

Телекомунікаційна система – організаційно-технічна система, яка забезпечує інформаційний обмін з використанням технічних і програмних засобів передаючи інформації у вигляді сигналів, знаків, звуків, зображень;

Інтегрована система - набір декількох взаємозв’язаних інформаційних та (або) ТКС, де функціонування певних з них залежить від результатів функціонування інших, коли цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Стандарт визначає процес побудови КСЗІ, як для новостворюваних систем, так і для вже існуючих, котрі вимагають впровадження або модернізації КСЗІ.

КСЗІ розроблена згідно до рекомендацій даного стандарту має складатися з заходів та засобів, які забезпечать захист інформації від:

* витоку технічними каналами, серед яких канали побічних електромагнітних випромінювань і наведень, акустико-електричні та інші види каналів;
* 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.

В НД ТЗІ 3.7-003 визначено ряд етапів створення та впровадження КСЗІ. Процес розробки починається з формулювання вимог до системи, що має бути побудована, обґрунтовується необхідність її створення, вивчення середовища в якому функціонує інформаційно-телекомунікаційна система. Результатом є перелік об’єктів захисту, потенційні загрози для інформації, модель загрози та порушника. В результаті формується авдання на створеня КСЗІ.

На другому етапі розробляється політика безпеки інформації в ІТС. З переліку варіантів побудови вибирається самий оптимальний. Пізніше відбувається оформлення політики безпеки, де вибираються рішення з протидії всім суттєвим загрозам, формування загальних вимог, правил та обмежень.

Результатом етапу зі створення технічного завдання на створення КСЗІ є документ, що визначає вимоги до захисту інформації, яка оброблюється в ІТС, порядок створення КСЗІ, порядок проведенн випробувань иа введення її в експлуатацію як частину ІТС.

На основі складеного ТЗ має проводитися розробка проекту КСЗІ, де обґрунтовуються і приймаються проектні рішення для реалізації вимог технічного завдання, розроблюється, оформлюється та затверджується робоча та експлуатаційна документація КСЗІ.

Наступним етапом є введення КСЗІ в експлуатацію та оцінка захищеності інформації в ІТС. Тут відбувається підготовка КСЗІ до введення в дію, навчання користувачів, роботи з розгортання системи, пусконалагоджувальні роботи, випробувальна екслуатація. Після дослідної експлуатації проводиться держана експертиза.

* + 1. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

Даний стандарт встановлює критерії для оцінки захищеності інформації, що оброблюється в комп’ютерних системах, від несанкціонованого доступу. Є базою для визначення вимог до захищених комп’ютерних систем і засобів захисту, оцінки ступеню захищеності інформації в системі та придатність систем для обробки критичної інформації.

Стандарт розлядає два види вимог при оцінці здатності комп'ютерної системи забезпечувати захист інформації, що оброблюється від неправомірного доступу, а саме:

* вимоги до функцій захисту
* вимоги до гарантій

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

Функціональні критерії поділено на чотири групи, де описано вимоги до послуг, які забезпечують захист від одного з типів загроз.

Групи функціональних критеріїв:

* Конфіденційність. Загрози, що пов’язані з несакціонованим перегдядом та ознайомленням з інформацією.
* Цілісність. Загрози, що зв’язані з несанкціонованою зміною фнформації.
* Доступність. Такі загрози, які порушують можливість використання комп’ютерних систем або інформації, що оброблюється.
* Спостережність. Розглядає ідентифікацію та контроль за діями користувача, керованість комп’ютерною системою.

Окремою ланкою виділено критерії гарантій, що дають змогу оцінити коректність реалізації послуг. До них належать вимоги до архітектури, середовища розробки, послідовності розробки, випробування комплексу засобів захисту та середовища функціонування.

Структуру критеріїв наведено на рисунку .



Рисунок

* + 1. НД ТЗІ 2.5-008-02 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»
  1. Стандарт BS 7799

Один з перших міжнародних стандартів управління інформаційної безпеки - британський стандарт BS 7799 - вже давно вийшов за національні рамки. Перша його частина, BS 7799-1 «Практичні правила управління інформаційною безпекою» - була розроблена в 1995 році Британським інститутом стандартів за замовленням уряду Великобританії.

Відповідно до цього стандарту будь-яка служба безпеки, ІТ-відділ, керівництво компанії повинні почати працювати згідно з загальним регламентом. Не важливо, йде мова про захист паперового документообігу або електронних даних. В даний час Британський стандарт BS 7799 підтримується в 27 країнах світу, в числі яких країни Британського Союзу, а також Швеція та Нідерланди. В 2000 г. Міжнародний інститут стандартів ISO на базі британського BS 7799 розробляв та випустив міжнародний стандарт управління безпекою ISO / IEC 17799. Сьогодні можна стверджувати, що BS 7799 та ISO 17799 це один і той же стандарт, що має сьогодні світове визнання та статус міжнародного стандарту ISO.

Перша частина стандарту "Управління інформаційною безпекою. Практичні правила", містить систематичний, вельми повний, універсальний перелік регуляторів безпеки, корисний для організації практично будь-якого розміру, структури і сфери діяльності. Вона призначена для використання в якості довідкового документа керівниками і рядовими співробітниками, що відповідають за планування, реалізацію і підтримку внутрішньої системи інформаційної безпеки.

Відповідно до стандарту, мета інформаційної безпеки - забезпечити безперервну роботу організації, по можливості запобігти і / або мінімізувати збиток від порушень безпеки.

Управління інформаційною безпекою дозволяє колективно використовувати дані, одночасно забезпечуючи їх захист і захист обчислювальних ресурсів.

Підкреслюється, що захисні заходи виявляються значно дешевшими і ефективними, якщо вони закладені в інформаційні системи і сервіси на стадіях завдання вимог і проектування.

Регулятори безпеки, визначені в першій частині BS7799 поділено на десять груп:

* політика безпеки;
* загальноорганізаційні аспекти захисту;
* класифікація активів і керування ними;
* безпека персоналу;
* фізична безпеки і безпека навколишнього середовища;
* адміністрування систем і мереж;
* керування доступом до систем і мереж;
* розробка і супровід інформаційних систем;
* керування безперебійною роботою організації;
* контроль відповідності вимогам

У стандарті виділяється десять ключових регуляторів, які або є обов'язковими відповідно до чинного законодавства, або вважаються основними структурними елементами інформаційної безпеки. До них відносяться:

* документ про політику інформаційної безпеки;
* розподіл обов'язків по забезпеченню інформаційної безпеки;
* навчання і підготовка персоналу до підтримки режиму інформаційної безпеки;
* повідомлення про випадки порушення захисту;
* антивірусні засоби;
* процес планування безперебійної роботи організації;
* контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
* захист документації;
* захист даних;
* контроль відповідності політиці безпеки.

У другій частині стандарту BS 7799-2: 2002 "Системи управління інформаційною безпекою - специфікація з керівництвом по використанню" предметом розгляду, як випливає з назви, є система управління інформаційною безпекою.

Під системою управління інформаційною безпекою (СУІБ) розуміється частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

В основу процесу управління покладена чотирьохфазна модель, що включає:

* планування;
* реалізацію;
* оцінку;
* коректування.

1. Дослідження сучасного стану та напрямки розвитку системи оцінки відповідності для СЗІ
   1. Глобальна інфраструктура якості

1. Дослідження вимог до інформаційних систем та їх реалізація у відповідності до ISO:15408
   1. Структура стандарту ISO:15408

Основні цілі, які було поставлено при розробці стандарта:

* Уніфікація національних стандартів в сфері оцінки безпеки інформаційних систем
* Підвищення рівня довіри до оцінки безпеки ІТ
* Зменшення витрат на проведення оцінки ІТ

Стандарт розділено на три частин:

* Частина 1: Введення та загальна модель
* Частина 2: Функціональні вимоги безпеки
* Частина 3: Вимоги гарантованості

Перша частина «Загальних критеріїв» містить визначення загальних понять, концепції, опис моделі і методики проведення оцінки безпеки ІТ. У ній вводиться понятійний апарат і визначаються принципи формалізації предметної області.

Вимоги до функціональності засобів захисту наводяться у другій частині «Загальних критеріїв» і можуть бути безпосередньо використані при аналізі захищеності для оцінки повноти реалізованих в ІС функцій безпеки.

Третя частина «Загальних критеріїв», поряд з іншими вимогами до адекватності реалізації функцій безпеки, містить клас вимог з аналізу вразливостей засобів і механізмів захисту під назвою AVA: Vulnerability Assessment. Даний клас вимог визначає методи, які повинні використовуватися для попередження, виявлення та ліквідації наступних типів вразливостей:

* Наявність побічних каналів витоку інформаціїї
* помилки в конфігурації, або неправильне використання системи, що призводить до переходу системи в небезпечний стан
* недостатня надійність (стійкість) механізмів безпеки, що реалізують відповідні функції безпеки
* наявність вразливостей («дірок») в засобах захисту інформації, що дозволяють користувачам отримувати несанкціонованого доступу до інформації в обхід існуючих механізмів захисту.

Основними відмітними рисами ОК є:

* Наявність певної методології і системи формування вимог і оцінки безпеки ІТ. Системність простежується починаючи від термінології і рівнів абстракції уявлення вимог і закінчуючи їх використанням при оцінці безпеки на всіх етапах життєвого циклу виробів ІТ;
* Загальні критерії, які характеризуються найбільш повною на сьогоднішній день сукупністю вимог безпеки ІТ
* чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. Функціональні вимоги відносяться до сервісів безпеки (ідентифікації, аутентифікації, управління доступом, аудиту і т.д.), а вимоги довіри - до технології розробки, тестування, аналізу вразливостей, експлуатаційної документації, постачання, супроводу, тобто до всіх етапів життєвого циклу виробів ІТ
* Критерії, що включають шкалу довіри до безпеки (оціночні рівні довіри до безпеки), яка може використовуватися для формування різних рівнів впевненості в безпечності продуктів ІТ
* Систематизація і класифікація вимог по ієрархії «клас - сімейство - компонент - елемент» з унікальними ідентифікаторами вимог, які забезпечують зручність їх використання
* Компоненти вимог в сімействах і класах, які ранжовані за ступенем повноти і жорсткості, а також згруповані в пакети вимог
* Гнучкість в підході до формування вимог безпеки для різних типів виробів ІТ і умов їх застосування забезпечуються можливістю цілеспрямованого формування необхідних наборів вимог у вигляді визначених у ОК стандартизованих структурах (профіляхй захисту і завдань з безпеки);
* відкриті для подальшого нарощування сукупності вимог

За рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ОК представляють найбільш досконалий з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку, являє собою не функціональний стандарт, а методологію завдання, оцінки та каталог вимог безпеки ІТ, який може нарощуватися і уточнюватися.

У певному сенсі роль функціональних стандартів виконують профілі захисту, які формуються з урахуванням рекомендацій та каталогу вимог ОК, але можуть включати і будь-які інші вимоги, які необхідні для забезпечення безпеки конкретного виробу або типу виробів ІТ.

* 1. Вимоги до архітектури інформаційної системи для забезпечення безпеки її функціонування

Ідеологія відкритих систем суттєво вплинула на методологічні аспекти і напрямки розвитку складних ІС. Вона базується на суворому дотриманні сукупності профілів, протоколів і стандартів де-факто і де-юре. Програмні і апаратні компоненти цієї ідеології повинні відповідати найважливішим вимогам переносимості та можливості узгодженої спільної роботи з іншими віддаленими компонентами. Це дозволяє забезпечити сумісність різних компонент інформаційних систем, а також засобів передачі даних. Завдання зводиться до максимально можливого повторного використання розроблених і апробованих програмних та інформаційних компонент при зміні обчислювальних апаратних платформ, ОС і процесів взаємодії.

При створенні складних, розподілених інформаційних систем, їх проектуванні архітектури, інфраструктури, виборі компонентів і зв'язків між ними слід враховувати крім загальних (відкритість, масштабованість, переносимість, мобільність, захист інвестицій тощо) ряд специфічних концептуальних вимог, спрямованих на забезпечення безпеки функціонування:

o архітектура системи повинна бути достатньо гнучкою, тобто повинна допускати відносно просте, без докорінних структурних змін, розвиток інфраструктури і зміна конфігурації використовуваних засобів, нарощування функцій і ресурсів ІС відповідно з розширенням сфер і завдань її застосування;

o повинні бути забезпечені безпека функціонування системи при різних видах загроз і надійний захист даних від помилок проектування, руйнування або втрати інформації, а також авторизація користувачів, керування робочої завантаженням, резервуванням даних і обчислювальних ресурсів, максимально швидким відновленням функціонування ІС;

o слід забезпечити комфортний, максимально спрощений доступ користувачів до сервісів і результатами функціонування ІС на основі сучасних графічних засобів, мнемосхем та наочних користувальницьких інтерфейсів;

o систему повинна супроводжувати актуалізована, комплектна документація, що забезпечує кваліфіковану експлуатацію і можливість розвитку ІС.

Підкреслимо, що системи безпеки, якими б потужними вони не були, самі по собі не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки перевірена архітектура здатна зробити ефективним об'єднання сервісів, забезпечити керованість інформаційної системи, її здатність розвиватися і протистояти новим загрозам при збереженні таких властивостей, як висока продуктивність, простота і зручність використання.

З практичної точки зору забезпечення безпеки найбільш важливими є наступні принципи побудови архітектури ІС:

o проектування ІС на принципах відкритих систем, дотримання визнаним стандартам, використання апробованих рішень, ієрархічна організація ІС з невеликим числом сутностей на кожному рівні - все це сприяє прозорості і хорошої керованості ІС;

o безперервність захисту в просторі і часі, неможливість подолати захисні засоби, виключення спонтанного або викликаного переходу в небезпечний стан - при будь-яких обставин, у тому числі позаштатних, захисне засіб або цілком виконує свої функції, або цілком блокує доступ до системи або її частина;

o посилення самої слабкої ланки, мінімізація привілеїв доступу, поділ функцій обслуговуючих сервісів і обов'язків персоналу. Передбачається такий розподіл ролей і відповідальності, щоб одна людина не може порушити критично важливий для організації процес або створити пролом у захисті з незнання або замовлення зловмисників. Стосовно до програмно-технічному рівню принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків. Це дозволяє зменшити шкоду від випадкових або навмисних некоректних дій користувачів та адміністраторів;

o ешелонування оборони, розмаїтість захисних засобів, простота і керованість інформаційної системи і системою її безпеки. Принцип ешелонування оборони наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати программнотехнические засоби, за ідентифікацією і аутентифікацією - управління доступом, протоколювання й аудит. Ешелонована оборона здатна не тільки не пропустити зловмисника, але і в деяких випадках ідентифікувати його завдяки протоколювання і аудиту. Принцип розмаїтості захисних засобів передбачає створення різних за характером оборонних рубежів, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками.

Дуже важливий загальний принцип простоти і керованості ІС в цілому і захисних засобів в особливості. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснювати централізоване адміністрування. У цьому зв'язку важливо відзначити інтегруючу роль web-сервісу, що ховає розмаїтість об'єктів, що обслуговуються, і надає єдиний, наочний інтерфейс. Відповідно, якщо об'єкти деякого виду (наприклад, таблиці бази даних) доступні через Інтернет, необхідно заблокувати прямий доступ до них, оскільки в противному випадку система буде вразливою, складною і погано керованою.

Продумана і впорядкована структура програмних засобів і баз даних, топології внутрішніх і зовнішніх мереж безпосередньо відбивається на що досягає якості і безпеки ІС, а також на трудомісткість їх розробки. При строгому дотриманні правил структурної побудови значно полегшується досягнення високих показників якості і безпеки, так як скорочується число можливих помилок в реалізують програмах, відмов і збоїв устаткування, спрощується їх діагностика і локалізація. У добре структурованої системи з чітко виділеними компонентами (клієнт, сервер додатків, ресурсний сервер) контрольні точки виділяються досить чітко, що вирішує задачу докази достатності застосовуваних засобів захисту і забезпечення неможливості обходу цих коштів потенційним порушником.

Високі вимоги, пропоновані до формування архітектури та інфраструктури на стадії проектування ІС, визначаються тим, що саме на цій стадії можна значною мірою мінімізувати число вразливостей, пов'язаних з непредумышленными дестабілізуючими факторами, які впливають на безпеку програмних засобів, баз даних і систем комунікації.

Аналіз безпеки ІС при відсутності злочинних факторів базується на моделі взаємодії основних компонентів ІС (рис. 1).

В якості об'єктів уразливості розглядаються:

o динамічний обчислювальний процес обробки даних, автоматизованої підготовки рішень і вироблення керуючих впливів;

o об'єктний код програм, виконуваних обчислювальними засобами в процесі функціонування ІС;

o дані та інформація, накопичена в базах даних;

o інформація, яка видається споживачам і на виконавчі механізми.



**Модель аналізу безпеки ІС при відсутності злочинних загроз**

### Етапи побудови системи безпеки ІС

Концепція інформаційної безпеки визначає етапи побудови системи інформаційної безпеки у відповідності зі стандартизованих життєвим циклом ІС: аудит безпеки (обстеження) існуючої системи захисту ІВ, аналіз ризиків, формування вимог і вироблення першочергових заходів захисту, проектування, впровадження, атестація, супровід системи. Розглянемо коротко зміст окремих етапів.

**Аудит безпеки.**Аудит безпеки може включати в себе, принаймні, чотири різні групи робіт.

До ***першої групи*** належать так звані тестові зломи ІС. Ці тести застосовуються, як правило, на початкових стадіях обстеження захищеності ІС. Причина малої ефективності тестових зломів ховається в самій постановці завдання. Дійсно, основним завданням зломщика є виявлення декількох вразливостей і їх використання для доступу в систему. Якщо тест виявився успішним, то, запобігши потенційний розвиток можливих сценаріїв злому, роботу треба починати спочатку і шукати такі. Неуспіх злому може означати в рівній мірі як захищеність системи, так і недостатність тестів.

***Друга група -*** експрес-обстеження. В рамках цього, звичайно нетривалої роботи оцінюється загальний стан механізмів безпеки в обстежуваній ІС на основі стандартизованих перевірок. Експрес-обстеження зазвичай проводиться у разі, коли необхідно визначити пріоритетні напрями, що дозволяють забезпечити мінімальний рівень захисту інформаційних ресурсів. Основу для нього складають списки контрольних питань, що заповнюються в результаті інтерв'ювання, так і тестової роботи автоматизованих сканерів захищеності.

***Третя група робіт з аудиту*** - атестація систем на відповідність вимогам захищеності інформаційних ресурсів. При цьому відбувається формальна перевірка набору вимог як організаційного, так і технічного аспектів, розглядаються повнота і достатність реалізації механізмів безпеки. Типова методика аналізу корпоративної інформаційної захищеності складається з сукупності наступних методів:

o вивчення вихідних даних за структурою, архітектури, інфраструктури та конфігурації ІС на момент обстеження;

o попередня оцінка ризиків, пов'язаних із здійсненням загроз відносно технічних та інформаційних ресурсів;

o аналіз механізмів безпеки організаційного рівня, політики безпеки організації і організаційно-распоряди

тельний документації щодо забезпечення режиму ІБ і оцінка їх відповідності вимогам існуючих стандартів і нормативних документів, а також їх адекватності існуючим ризикам;

o аналіз конфігураційних файлів маршрутизаторів і Ргоху-серверів, поштових і DNS-сервери (Domain Name System), шлюзів віртуальних приватних мереж (VPN), інших критичних елементів мережевої інфраструктури;

o сканування зовнішніх мережевих адрес локальної мережі;

o сканування ресурсів локальної мережі зсередини;

o аналіз конфігурації серверів і робочих станцій з допомогою спеціалізованих програмних агентів.

Перераховані технічні методи передбачають застосування як активного, так і пасивного тестування системи захисту. Активне тестування полягає в моделюванні дій потенційного зловмисника; а ***пасивне -*** передбачає аналіз конфігурації ОС і додатків за шаблонами з використанням списків перевірки. Тестування може проводитися вручну або з використанням спеціалізованих програмних засобів.

При аналізі конфігурації засобів захисту для зовнішнього периметра локальної мережі і управління міжмережними взаємодіями особлива увага звертається на наступні аспекти:

o налаштування правил розмежування доступу (фільтрація мережевих пакетів);

o схеми та налаштування параметрів аутентифікації;

o настройка параметрів системи реєстрації подій;

o використання механізмів, що забезпечують приховування топології мережі, яка захищається (наприклад, трансляція мережевих адрес);

o налагодження механізмів оповіщення про атаки і реагування;

o наявність і працездатність засобів контролю цілісності;

o версії використовуваного ЗА і встановлені оновлення.

Аналіз конфігурації передбачає перевірку правильності установки сотень різних параметрів. Для автоматизації цього процесу можуть використовуватися спеціалізовані програмні засоби аналізу захищеності, вибір яких в даний час досить широкий.

Один із сучасних і швидко розвиваються методів автоматизації процесів аналізу і контролю захищеності розподілених комп'ютерних систем - використання технології інтелектуальних програмних агентів. На кожну з контрольованих систем встановлюється програмний агент, який виконує відповідні налаштування, перевіряє їх правильність, контролює цілісність файлів, своєчасність установки оновлень, а також вирішує інші завдання з контролю захищеності ІС. Управління агентами здійснює по мережі програма-менеджер. Такі менеджерм, які є центральними компонентами таких систем, посилають керуючі команди всім агентам контрольованого ними домену і зберігають всі отримані від агентів дані в центральній БД. Адміністратор керує менеджерами за допомогою графічної консолі, що дозволяє вибирати, змінювати та створювати політики безпеки, аналізувати зміни стану системи, здійснювати ранжування вразливостей і т. п. Все взаємодії між агентами, менеджерами і керуючої консолі здійснюються по захищеному клієнт-серверному протоколу. Такий підхід, наприклад, використаний при побудові комплексної системи управління безпекою організації ESM (виробник - компанія "Symantec Enterprise Security Manager").

***Четверта група -*** перед проектне обстеження - самий трудомісткий варіант аудиту. Такий аудит передбачає аналіз організаційної структури підприємства в додатку до ІР, правила доступу співробітників до тих або іншим додаткам. Потім виконується аналіз самих додатків. Після цього повинні враховуватися конкретні служби доступу з одного рівня на інший, а також служби, необхідні для інформаційного обміну. Потім картина доповнюється вбудованими механізмами безпеки, що в поєднанні з оцінками втрат у разі порушення ІБ дає підстави для ранжирування ризиків, які існують в ІС, і вироблення адекватних контрзаходів. Успішне проведення передпроектного обстеження, подальшого аналізу ризиків і формування вимог визначають, наскільки прийняті заходи будуть адекватні погрозам, ефективні і економічно виправдані.

**Проектування системи.**В даний час склалися два підходи до побудови системи ІБ: продуктовий і проектний. В рамках ***продуктового*** підходу вибирається набір засобів фізичної, технічної і програмної захисту (готове рішення), аналізуються функції, а на основі аналізу функцій визначається політика доступу в робочі та технологічні приміщення, до інформаційних ресурсів. Можна надходити навпаки: спочатку опрацьовується політика доступу, на основі якої визначаються функції, необхідні для її реалізації, і здійснюється вибір засобів і продуктів, що забезпечують виконання цих функцій. Вибір методів залежить від конкретних умов діяльності організації, її місцезнаходження, розташування приміщень, складу підсистем ІС, сукупності розв'язуваних завдань, вимог до системи захисту і т. д. Продуктовий підхід більш дешевий з точки зору витрат на проектування. Крім того, в деяких випадках він є єдино можливим в умовах дефіциту рішень або жорстких вимог нормативних документів на державному рівні (наприклад, для криптографічного захисту інформації в мережах спеціального призначення та урядових телефонних мережах застосовується тільки такий підхід). ***Проектний*** підхід свідомо більш повний, і рішення, побудовані на його основі, зручніша і простіше аттестуемы. Він краще і при створенні великих гетерогенних розподілених систем, оскільки на відміну від продуктового підходу не пов'язаний спочатку з тією чи іншою платформою. Крім того, він забезпечує більш "довгоживучі" рішення, оскільки допускає проведення заміни продуктів і рішень без зміни політики доступу. Це, в свою чергу, забезпечує хороший показник повернення інвестицій (ROI) при розвитку ІС і системи ІБ.

**Об'єкти або програми?**При проектуванні архітектури системи інформаційної безпеки застосовуються об'єктний, прикладної або змішаний підходи.

***Об'єктний*** підхід будує захист інформації на підставі фізичної структури того чи іншого об'єкта (будівлі, підрозділу, підприємства). Застосування об'єктного підходу припускає використання набору універсальних рішень для забезпечення механізмів безпеки, підтримують однорідний набір організаційних заходів. Класичним прикладом такого підходу є побудова захищених інфраструктур зовнішнього інформаційного обміну, локальної мережі, системи телекомунікацій і т. д. До його недоліків відносяться очевидна неповнота універсальних механізмів, особливо для організацій з великим набором складно пов'язаних між собою програм.

***Прикладний*** підхід "прив'язує" механізми безпеки до конкретного додатка. Приклад такого підходу - захист підсистеми або окремих зон автоматизації (бухгалтерія, склад, кадри, проектне бюро, аналітичний відділ, відділи маркетингу і продажів тощо). При більшій повноті захисних заходів такого підходу у нього є і недоліки, а саме: необхідно пов'язувати різні за функціональним можливостям засоби безпеки для мінімізації витрат на адміністрування та експлуатацію, а також задіяти вже існуючі засоби захисту інформації для збереження інвестицій.

Можлива комбінація двох описаних підходів. У ***змішаному*** підході ІС представляється як сукупність об'єктів, для кожного з яких застосовано об'єктний підхід, а для сукупності взаємозалежних об'єктів - прикладної. Така методика виявляється більш трудомісткою на стадії проектування, однак часто дає хорошу економію коштів при впровадженні, експлуатації та супроводу системи захисту інформації.

**Служби і механізми безпеки.**Стратегію захисту можна реалізувати двома методами: ресурсним і сервісним. Перший метод розглядає ІС як набір ресурсів, які "прив'язуються" до конкретних компонентів системи ІБ. Цей метод хороший для невеликих ІС з обмеженим набором завдань. При розширенні кола завдань і розростанні ІС доводиться багато в чому дублювати елементи захисту для однотипних ресурсів, що часто призводить до невиправданих витрат. Сервісний підхід трактує ІС як набір служб, програмних і телекомунікаційних сервісів для надання послуг користувачам. У цьому випадку один і той же елемент захисту можна використовувати для різних сервісів, побудованих на одному і тому ж або технічному пристрої. Сьогодні сервісний підхід видається кращим, оскільки він припускає строгий функціональний аналіз існуючих численних служб, що забезпечують функціонування ІС, і дозволяє виключити широкий клас загроз за допомогою відмови від "зайвих" служб і оптимізації роботи залишилися, роблячи структуру системи ІБ логічно обґрунтованою. Саме сервісний підхід лежить в основі сучасних стандартів щодо безпеки, зокрема ISO 15408.

**Впровадження та атестація.**Етап впровадження включає в себе комплекс послідовно проведених заходів, у тому числі установку і конфігурування засобів захисту, навчання персоналу роботі із засобами захисту, проведення попередніх випробувань і здачу в дослідну експлуатацію. Дослідна експлуатація дозволяє виявити і усунути можливі недоліки функціонування підсистеми інформаційної безпеки, перш ніж запустити систему в "бойовій" режим. Якщо в процесі дослідної експлуатації виявлені факти некоректної роботи компонентів, проводять коригування налаштувань засобів захисту, режимів їх функціонування і т. п. За результатами дослідної експлуатації вносять коригування (за необхідності) і уточнюють налаштування засобів захисту. Далі слід проведення приймально-здавальних випробувань, введення в штатну експлуатацію і надання технічної підтримки і супроводу.

Підтвердження функціональної повноти системи безпеки і забезпечення необхідного рівня захищеності ІС забезпечується проведенням атестації системи ІБ відповідним акредитованим центром Федеральної служби з технічного та експортного контролю або зарубіжної незалежною лабораторією. Атестація передбачає комплексну перевірку захищеного об'єкта в реальних умовах експлуатації для оцінки відповідності застосовуваного комплексу заходів і засобів захисту необхідному рівню безпеки. Атестація проводиться згідно зі схемою, що складається на підготовчому етапі виходячи з наступного переліку робіт:

* аналіз вихідних даних, попереднє ознайомлення з атестуються об'єктом та інформатизації;
* експертне обстеження об'єкта інформатизації та аналіз документації з питань захисту інформації на предмет відповідності вимогам;
* o випробування окремих засобів і систем захисту інформації на аттестуемом об'єкті за допомогою спеціальної контрольної апаратури і тестових засобів;
* випробування окремих засобів і систем захисту інформації у випробувальних центрах (лабораторіях);
* комплексні атестаційні випробування об'єкта інформатизації в реальних умовах експлуатації;
* аналіз результатів експертного обстеження та атестаційних випробувань і затвердження висновку за результатами атестації об'єкта інформатизації.

За результатами випробувань готується звітна документація, проводиться оцінка результатів випробувань і видається атестат відповідності встановленого зразка. Його наявність дає право обробки інформації зі ступенем конфіденційності та на період часу, встановленими в атестаті.

**Технічна підтримка та супровід.**Для підтримки працездатності підсистеми інформаційної безпеки та безперебійного виконання їй своїх функцій необхідно передбачити комплекс заходів з технічної підтримки та супроводу програмного і апаратного забезпечення підсистеми інформаційної безпеки, включаючи поточне адміністрування, роботи, що проводяться в екстрених випадках, а також періодично проводяться профілактичні роботи. Цей комплекс заходів включає в себе:

* адміністрування штатних засобів захисту та їх технічне обслуговування;
* контроль стану системи, профілактичне обстеження конфігурації, виявлення потенційних проблем;
* моніторинг та встановлення випущених оновлень і програмних корекцій засобів захисту, а також використовуваних ОС, СУБД і додатків;
* регулярний пошук і аналіз вразливостей в захищається системі з використанням спеціальних засобів сканування;
* діагностику несправностей та проведення відновних робіт при виникненні аварійних і позаштатних ситуацій;
* періодичне тестування системи інформаційної безпеки та оцінка ефективності захисту.

Технічна підтримка та супровід системи інформаційної безпеки вимагає наявності у обслуговуючого персоналу певних знань і навичок і може здійснюватися як штатними працівниками організації - власника ІВ, відповідальними за інформаційну безпеку, так і співробітниками спеціалізованих організацій.