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;
* Германський стандарт BSI;
* Британський 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**, [англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *National Bureau of Standards. NBS*) — 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" \o "Стандартизація) 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" \o "Стандартизація) 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" \o "Стандарт) 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.

"Помаранчева книга" пояснює поняття безпечної системи, яка "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 "Помаранчевої 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".

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.
  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