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 конкретний стан систем, пов’язаних з обробкою та зберіганням даних, при якому забезпечується конфіденційность, цілісность та доступность останніх.

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** — національний орган США, відповідальний за  стандартизацію.

NIST — некомерційна та не пов'язана з урядом організація, яка координує роботи, пов'язані з добровільною стандартизацією в приватному секторі економіки, слідкує за діяльністю організацій, що розробляють стандарти та приймає рішення щодо надання стандартам статусу національних (у випадку, коли в ньому є зацікавленість з боку різних фірм і стандарт стає міжгалузевим).

NIST це єдина організація в США, яка приймає (затверджує) стандарти національного рівня. Основним завданням NIST є допомога у вирішенні проблем, загальнодержавного значення (забезпечення економії енергоресурсів, захист оточуючого середовища, підвищення рівня безпеки життя людини і умов на виробництві).

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, та інструкції щодо того, як їх правильно використовувати. Всі контролі в даному стандарті поділено на сімейства, які відповідають різним сферам забезпечення інформаційної безпеки. Сімейства контролів, якими керується 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 оцінювання безпеки |
| CM | Configuration Management | Керування конфігурацією |
| CP | Contingency Planning | Планування неперервності бізнесу |
| IA | Identification and Authentication | Ідентифікація та автентифікація |
| IR | Incident Response | Реакція 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 | Оцінювання 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 системи та інформації |
| PM | Program Management | Керування програмою ІБ |

Опис конжного контроля підпорядкований шаблону. Перш за все зазначено код сімейства контролів та його номер, наприклад, AU-2. Далі вказано його назву.

Основна частина складається з наступних розділів:

* Control. Опис специфічних дій або активностей, які виконуються організацією або ІС та мають відношення до забезпечення безпеки. Для певних контролів передбачено можливость гнучкого налаштування, яке надає можливість для організацій визначати окремі з параметрів, пов'язаних з контролем. Для прикладу, в ролі такого параметра може бути частота проведення аудитів, тривалість зберігання журналу логування або кількість спроб користувачів авторизуватися, що закінчились невдачею. Це дозволяє підлаштовувати контролі під потреби конкретной організації, спираючись на вимоги, запропоновані до забезпечення безпеки зі сторони цілей поставлених організацією, результатів оцінок рівня ризику та прийнятності його, також можна розглядати вимоги з боку закону і регуляторів.
* Supplemental Guidance. Додаткові відомості для певного контроля. Включає в себе роз'яснювальну інформацію стосовно імплементації та використання контролю і т.д. Додатково можна зазначити посилання на пов'язані з ним контролі.
* Control Enhancements. Дана секція визначає можливості для «покращення» контролів, додаючи до нього додаткову функціональность.
* References. Включає в себе посилання на закони, нормативні акти і т.д.
* Priority and Baseline Allocation. Має вигляд таблички, в якій зведено інформацію щодо рекомендованого пріоритету в ході прийняття рішеннь про реалізацію контролів і стартовий розподіл контролів серед базових наборів для систем з різними рівнями критичності. Пріоритизація імплементації дає змогу організаціям проводити реалізацію контролів ефективніше та в правильній послідовності, спочатку імплементуючи основоположні заходи.

Для впорядкування та забезпечення структурності підходу проведено розподіл контролів за різними типами. Він залежить від призначення контроля:

* Common. Загальні контролі, такі, що можуть бути успадкованими різноманітними системами і можуть бути використаними поза межами окремої ІС. Контроль безпеки успадковується в тому разі, коли він виконує свої функції безпеки в ІС, проте був розроблений, реалізований, оцінений, авторизований за межами цієї ІС
* System-specific. Контроль створено та реалізованоконкретної для використання в конкретній ІС.
* Hybrid. Контроль частково функціонує як загальний, і частково в ролі специфічного для системи.

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

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

Даний стандарт розроблений Міністерством оборони США. Він 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 використовуючи який можна було б оцінити ступінь довіри до обчислювальної системи розглядаючи 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" дає наступне визначення безпечної системи, як такої, що "використовуючи відповідні засоби курує доступом до інформаційних ресупсів, таким чином, щоб отримували право на читання, записування, створення та видалення інформації мали лише авторизовані користувачі або процеси, які працюють від їх імені ".

В "Помаранчевій книзі" довірену систему визначено як "систему, що використовує необхідні апаратні та/або програмні засоби, для забезпечення одночасної обробки інформаційних потоків різних ступенів секретності групами користувачів не порушуючи права на доступ". 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.

Розглянуті Критерії оцінюють, як безпеку, так і довіру тільки в площині управління доступом до даних, що являється засобом забезпечення конфіденційності і цілісності (статичності). Проблеми доступності в "Помаранчевій книзі" не розглядаються.

Найважливішими критеріями для оцінки ступеню довіри є:

* Політика безпеки – перелік правил поведінки, що описують те, яким чином організації обробляють, захищають і поширюють інформацію. Наприклад, вони визначають, випадки, коли користувачі можуть працювати з конкретним набором даних. З підвищенням ступіню довіри до системи, мають ставати суворішими та різноманітнішими політики безпеки. В залежності від політики, яка сформульована є можливість обирати конкретний механізм забезпечення безпеки. Політика безпеки являється активним аспектом захисту, який містить в собі аналіз вірогідних загроз і перелік дій для боротьби з ними.
* Рівнем гарантованості є ступінь довіри, який можна надати для архітектури та реалізації ІС. Довіра безпеки виникає за результатами тестування або після перевірки основного задуму та реалізації системи або компонент, з яких вона складається. Рівень гарантованості вказує на те, чи відповідають нормам обрані механізми, відповідальні за реалізацію політики безпеки. Являється пасивним аспектом захисту.

Вимоги, що пред'являються до інформаціної системи в ході процесу оцінювання, можна поділити на наступні типи вимог: націлені на впровадження послідовної політики безпеки, до ведення обліку використання системи, довіри до системи та вимоги до ведення документації на систему.

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

* группа Д - Minimal Protection (мінімальний захист) - об'єднує інформаційні системи, які не можуть задовольнити вимогам безпеки більш високих класів. В даном випадку група та клас співпадають;
* група С - Discretionary Protection (виборчий 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 (виборчий 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 цільовому середовищу, де планується її використовувати.

Основні характері риси Загальних критеріїв зазначено нижче:

* Вони зібрали нйбільш повну на сьогодні сукупність вимог до безпеки інформаційних технологій.
* Чітко поділяють вимоги безпеки на функціональні та вимоги довіри до безпеки. Функціональні треба асоціювати з функціями безпеки (ідентифікація, аутентифікація, управління доступом, аудит і т.д.). Вимоги ж довіри з технологіями розробки, перевірки, аналізу вразливостей, постачання, підтримки, іншими словами з усіма етапами життєвого циклу інформаційних технологій.
* Систематизує та класифікує вимоги згідно до ієрархії "клас" - "сімейство" - "компонент" - "елемент", використовуючи унікальні ідентифікатори вимог, що забезпечує зручне їх використання.
* Ранжирує компоненти вимог в родинах і класах відповідно зі ступенем повноти та жорсткості, групує їх в пакети функціональних вимог і оціночні рівні довіри.
* Додає гнучкість і динамізм в задачі задання вимог безпеки до різних видів інформаційних технологій та умов їх використання, що можна забезпечити шляхом формування переліку обов’язкових вимог у вигляді визначеному в ЗК стандартизованих структур (профілів захисту і завдань з безпеки).
* Відкритість для подальшого нарощування переліку вимог.

Предметом розгляду в ЗК є програмно-технічні та технологічні способи 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 перехоплення інформації в технічних каналах, 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 ЗК 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.

Фахівці в сфері інформаційної безпеки, визнають Загальні критерії, з його універсальністю, гнучкістю, деталізацією, повнотою та рівнем систематизації, як один з найдосконаліших стандартів в галузі. Враховуючи особливост пов'язані з його побудовою, можна сказати, що він має практично необмежені можливості до розвитку та представляє собою базовий стандарт, який містить методологію опису вимог безпеки ІТ, а також систематизований перелік 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 р. в Німеччині було опубліковано "Керівництво по захисту інформаційних технологій для базового рівня". Пізніше він був представлений як стандарт BSI. В основу покладено загальну методологію та компоненти керування інформаційною безпекою, які наведено нижче:

* Загальний спосіб управління безпекою інформації (організація системи менеджменту у сфері інформаційної безпеки)
* Опис компонент ІТ
* Найважливіші компоненти (рівень процедур, організація дій, повязаних з захистом, планування дій в форсмажорних випадках)
* Інфраструктура
* Різнотипні компоненти клієнтів (такі як: DOS, Windows, UNIX, мобільні девайси та інше)
* Різні види мереж («точка-точка», Novell NetWare, побудовані на базі OC UNIX і Windows, різнорідні мережі)
* Різні компоненти системи передачі даних (такі як комутатори, модеми, роутери та інше).
* Телекомунікаційні системи
* Стандартне ПО
* Бази даних
* Визначення головних компонент налагодження режиму інформаційної безпеки.
* Параметри об'єктів, які підлягають інформатизації
* Опис доступних інформаційних ресурсів певної компанії(до них відносять, для прикладу, апаратне і програмне забезпечення, таке як комп’ютери та сервери під керуванням ОС DOS, Windows або UNIX)
* Параметри комп’ютерних мереж заснованих на різних технологіях
* Технічні характеристики ТК обладнання (враховується як активне, так і пасивне)
* Вичерпні каталоги з переліком загроз безпеці та заходами контролю (кожний визначає більш ніж 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 ІТС. Це така система, що належить до якоїсь із перелічених далі систем: ІС, ТК система, інтегрована система.

ІС це система, що поєднує організаційні та технічні аспекти і в якої реалізовано технології обробки інформації, які використовують засоби обчислювальної техніки та ПЗ;

ТКС система, яка забезпечує обмін інформацією за допомогою технічних і програмних засобів, та в якій інформація має вигляд сигналів, знаків, звуків, зображень;

Інтегрована система набір декількох взаємозв’язаних ІС та/або ТКС, де робота певних з них залежна від результату роботи інших, у випадку, якщо їх поєднання під час роботи можна розглянути як одну цілу систему.

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

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

* Потрапляння її до технічних каналів, наприклад, до каналів побічних ЕМВ і наведень, акустико-електричні та інші види каналів;
* неправомірного доступу до інформаційних ресурсів з метою використати її, який може бути здійснено методом підключення до лінії зв’язку або приладів даної лінії, видавання себе як авторизованого користувача;
* впливів на дані, які можуть бути здійснені формуванням полів та сигналів, що має на меті порушити цілісность інформації та/або подолання системи захисту.

В НД ТЗІ 3.7-003 визначено ряд етапів проектвання та впровадження КСЗІ. Процес розробки починається з формулювання вимог до системи, що має бути побудована, обґрунтовується необхідність її створення, вивчення середовища в якому функціонує ІТС. Результатом є перелік об’єктів, що мають бути захищеними, перелік потенційних загроз для даних, моделі загроз та порушників. В результаті формується авдання на створеня КСЗІ.

На другому етапі розробляються політики інформаційної безпеки в ІТС. З переліку варіантів побудови вибирається самий оптимальний. Пізніше відбувається оформлення політики безпеки, де вибираються способи захисту від усіх суттєвих загроз, формуються загальні вимоги, правила та обмеження.

В результаті отримують документ, який описує вимоги щодо захисту інформації, оброблюваної в ІТС, послідовність створення КСЗІ, проведення випробувань та фнтеграції до складу ІТС.

На основі складеного ТЗ проводять розробку проекту КСЗІ, під час чого відбувається обґрунтування та прийняття проектних рішень для реалізації вимог, зазначених в технічному завданні, розроблюється, оформлюється та затверджується робоча та експлуатаційна документація КСЗІ.

Наступним етапом є введення КСЗІ в експлуатацію та оцінювання ступеню захищеності даних в ІТС. Тут відбуваються підготовчі роботи для переведення системи в робочий стан, навчання персоналу, роботи з розгортання системи, пусконалагоджувальні роботи, випробувальна екслуатація. Після дослідної експлуатації проводиться державна експертиза.

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

Даний стандарт визначає перелік критеріїв, використовуваних при оцінці рівня захищеності інформації, яка оброблюється в інформаційних системах, при спробах неправомірного доступу. Являється основою для визначення вимог до ІС і засобів захисту, оцінки рівня захищеності даних в таких системах та їх придатність для роботи з критичною інформацією.

Стандарт розглядає два види вимог при оцінці здатності ІС провадити захист інформації, що оброблюється, при спробах неправомірного доступу, а саме вимоги:

* до функції захисту
* до гарантій

Критерії розглядають ІС 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.

Для зручност зіставлення проведено поділ функціональних критеріїв на чотири групи:

* Критерії конфіденційності. Загрози, що пов’язані з несакціонованим перегдядом інформації.
* Критерії цілісності. Загрози, які зв’язані з несанкціонованою зміною інформації.
* Доступність. Такі загрози, які порушують можливість використання ІС або інформації, що оброблюється.
* Критерії спостережності. Розглядає ідентифікацію та контроль за діями користувача, керованість комп’ютерною системою.

Кожна група описує вимоги до сервісів, які впроваджують захист від конкретного типу загрози.

Окремою ланкою виділено критерії гарантій, які дають змогу кількісно оцінити коректність впровадження послуг. До них можна віднести вимоги до архітектури рішення, середовища розробки, послідовності розробки, випробування системи захисту та середовища функціонування.

Структурне представлення критеріїв наведено на рис.



Рисунок

* 1. Стандарт BS 7799

Британський стандарт BS 7799 це один з перших міжнародних стандартів управління інформаційною безпекою. Перший його розділ, BS 7799-1 «Практичні правила управління інформаційною безпекою» - був розроблений в 1995 році Британським інститутом стандартів за замовленням уряду Великобританії.

Відповідно до стандарту будь-яка служба безпеки, ІТ-відділ, вищий менеджмент компаній мають почати працювати у відповідності з загальним регламентом. Не важливо, буде відбуватись захист паперових документів чи електронних даних. Зараз стандарт BS 7799 підтримують в 27 країнах світу. В 2000 році Міжнародний інститут стандартів ISO розробив міжнародний стандарт управління безпекою ISO / IEC 17799, спираючись на BS 7799. Зараз можна побачити, що BS 7799 та ISO 17799 мають однаковий сенс та визнаний у світі.

Перша частина "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 захисту інформації.

Згідно зі стандартом, мета інформаційної безпеки - забезпечити безперервну роботу організації, по можливості запобігти і/або мінімізувати збиток від порушень безпеки.

Управління інформаційною безпекою дозволяє сумісно користуватися даними, одночасно забезпечуючи захист самих даних та 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;
* розробка і пыдтримка інформаційних систем;
* керування безперебійною роботою організацій;
* контроль на відповіднысть вимогам

У стандарті виділяється десять ключових регуляторів, які або є обов'язковими відповідно до чинного законодавства, або їх прийнято як основні структурні елементи інформаційної безпеки. До них відносяться:

* документ про політику інформаційної безпеки;
* поділ зобов'язань із забезпечення інформаційної безпеки;
* навчання і підготовка працівників, які підтримуватимуть режим інформаційної безпеки;
* сигналізація при випадках порушення захисту;
* антивірусні засоби;
* процес планування безперервної роботи організацій;
* нагляд за створенням копій ПЗ, котре захищене авторськими правами;
* захист супровідних документів;
* захист даних;
* контроль за відповідністю до політики безпеки.

Друга частина BS 7799-2: 2002 "Системи управління інформаційною безпекою" розглядає систему управління інформаційною безпекою. Під якою мається на увазі частина всієї системи управління, яка опирається на аналіз ризиків і основним призначенням якої є проектування, реалізація, контроль, підтримка та вдосконалення заходів у сфері ІБ. Дана система складається з організаційних структур, політик, дій по плануванню, обов'язків, процедур, процесів і ресурсів.

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

Основними цілями, які було поставлено при розробці даного стандарту:

* Зведення стандартів в сфері оцінки захищеності ІС до уніфікованого вигляду
* Підняти ступінь довіри оцінці захищеності ІТ
* Мінімізація витрат на оцінювання ІТ

Стандарт розділено на три частини:

* Введення та загальна модель
* Функціональні вимоги безпеки
* Вимоги щодо гарантій

У першій частині «Загальних критеріїв» містяться визначення основних понять, концепції, опис моделей та методик проведення оцінок захищеності ІТ. В ній введено основні поняття та визначено принципи щодо того як формалізувати предметну область.

В другій частині наведено вимоги до функціональної складової засобів захисту. Їх можна використати для аналізу захищеності та для оцінки повноти реалізації функцій безпеки в проектованій системі.

В третій частині міститься клас вимог щодо аналізу вразливостей засобів захисту, що називається AVA: Vulnerability Assessment. Цей клас описує методи, які треба використовувати щоб попередити, виявити і ліквідувати наступні типи вразливостей:

* існування каналів, що призводять до витоку даниї
* конфігураційні помилки, або використання систем, невірним шляхом, що може призвести до переходу її в небезпечний стан
* низька надійність засобу забезпечення безпеки, який реалізує відповідну функцію безпеки
* наявність вразливих точок в механізмах захисту інформації, які можуть дозволити користувачу отримати несанкціонований доступ до інформації, обходячи існуючі механізми захисту.

Основні відмітні риси ОК:

* використання визначених методологій ти системи створення вимог при оцінці захищеності ІТ. Можна простежити системність починаючи з термінів та рівнів абстракції вимог до того як вони використовуються при проведенні оцінки захищеності на всіх етапах життєвого циклу системи;
* містять в собі найбільш повну на сьогодні сукупність вимог щодо безпеки ІТ
* чітко поділяють вимоги безпеки на вимоги до функціональних частин та вимоги довіри до безпеки. Вимоги до функціональних компонент відносять до сервісів безпеки, а вимоги довіри - до технологій розробки, проведення перевірки, аналізу вразливостей, передачі користувачам, підтримки, іншими словами до кожного з етапів життєвого циклу системи
* в склад стандарту включено шкалу довіри до безпеки, яку можна використати при створенні різних рівнів упевненості в безпечності систем
* вони систематизують і класифікують вимоги згідно з ієрархією «клас - сімейство - компонент - елемент» використовуючи унікальні ідентифікатори вимог, що забезпечує зручне їх використання
* ранжування компонентів вимог в сімействах і класах за ступенем повноти і жорсткості, і групування в пакети вимог
* відкриті для подальшого нарощування сукупності вимог

В порівнянні з іншими стандартами, по рівню систематизованості, здатності поглибити деталізацію вимог та їх повноті, ISO: 15408 можна визнати одним із самих досконалих серед існуючих зараз стандартів. При цьому, зважаючи на особливості його побудови, можна зазначити, що стандарт має багато можливостей для продовження розвитку. ISO:15408 являється не просто функціональним стандартом, а методологією завдання, оцінки та перелік вимог безпеки ІТ, який можна нарощувати та уточнювати.

* 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.

1. Розрахунок кількісного показника захищеності інформації від несанкціонованого доступу в автоматизованих системах

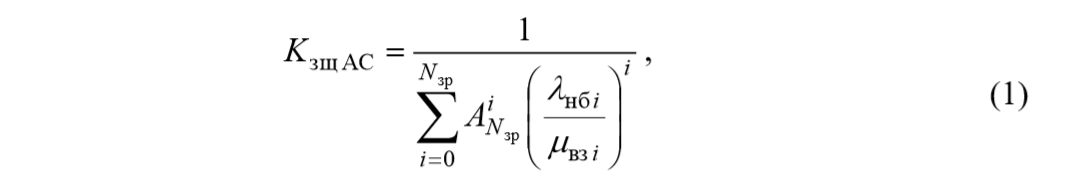
Насьогодні більшість норматиних документів передбачає проведення оцінки захищеності автоматизованої системи від несанкціонованого доступу за якісним критерієм, з орієнтацією на статичні умови фунціонування систем захисту.

Для атестації АС і сертифікації засобів обчислювальної техніки відповідно до вимог чинних нормативних документів необхідні висока кваліфікація персоналу, обробка великих обсягів даних і значні витрати часу. У відомих вітчизняних та зарубіжних методик кількісного оцінювання захищеності інформації (підхід на основі аналізу інформаційних ризиків, підхід на основі моделі системи забезпечення безпеки Клементса) є ряд недоліків, що не дозволяють безпосередньо використовувати їх для оцінки захищеності, а саме:

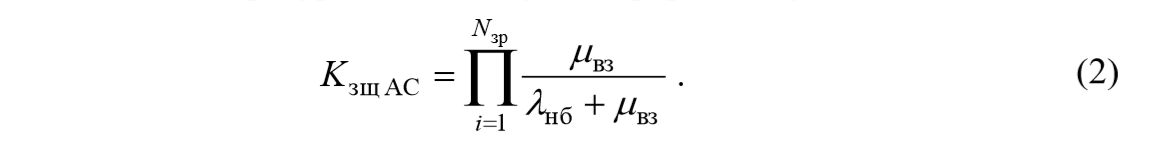
* не враховується реальна структура АС;
* оцінюється вартість втрат від несанкціонованого доступу до інформації в грошових одиницях, що прийнятно не для всіх АС;
* не повністю враховуються варіативність сценаріїв реалізації НСД і динамічні характеристики процесу захисту інформації.

Захищеність інформації в АС від НСД визначається захищеністю її ресурсів. Для оцінки захищеності доцільно використовувати її комплексні показники, що враховують і процеси порушення безпеки ресурсів в АС, і процеси контролю і відновлення їх захищеного стану. В якості такого показника пропонується використовувати коефіцієнт захищеності інформації АС від НСД, аналогічний використовуваному в теорії надійності коефіцієнту готовності.

При наявності можливості відновлення захищеності тільки одного ресурсу для розрахунку коефіцієнта захищеності інформації від несанкціонованого доступу в АС може використовуватися наступна формула:

Де Nзр – кількість ресурсів, що підлягають захисту, ANзрі  – кількість розміщень з Nзр по *i*, λнб – інтенсивність порушень безпеки ресурсів, µвз – інтенсивність відновлення захищеності ресурсів.

При умовно необмежені можливості по відновленню захищеності ресурсів використовувана формула буде мати вигляд:



Проведемо порівняльний аналіз захищеності інформації від несанкціонованого доступу на прикладі трьох АС, побудованих на основі локальних обчислювальних мереж і відрізняються масштабом і можливостями системи захисту. Кожен співробітник організації має робочу станцію, під керуванням ОС Windows, на якій знаходяться його користувацькі дані. Робочі станції об'єднані в обчислювальну мережу з декількома серверами, під керуванням ОС Windows Server, на яких функціонують поштовий сервер, СУБД, Web-сервер підприємства, миттєва система обміну повідомлень для співробітників і т. д. Нехай АС першого підприємства має 50 критично важливих захищених ресурсів (5 загальних ресурсів, розташованих на серверах, 45 ресурсів – дані користувачів на їх робочих станціях), АС другого підприємства має 100 критично важливих ресурсів, що захищаються (10 загальних ресурсів, 90 ресурсів – дані користувачів), АС третього підприємства має 150 критично важливих ресурсів, що захищаються (15 загальних ресурсів, 135 ресурсів – дані користувачів).

У розрахунку на найгірший випадок припустимо, що порушник «ідеальний» (має високу кваліфікацію, постійно відстежує появу нових вразливостей, а також має можливість миттєво використовувати їх для здійснення несанкціонованого доступу до інформації, що обробляється в АС розглянутих організацій). При використанні такої моделі порушника інтенсивність порушень безпеки інформації АС відповідає інтенсивності появи вразливостей в програмному забезпеченні АС. Аналіз загальнодоступною статистики по виявленню вразливостей в АС на основі ОС Windows показав, що інтенсивність в середньому становить дев'ять порушень безпеки в місяць, тобто λнб = 0,013 / год.

Зазвичай адміністратор безпеки АС організації може в кожен момент часу відновлювати захищеність лише одного ресурсу. Тоді, використовуючи формулу (1), можна отримати залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення її захищеності в даних умовах

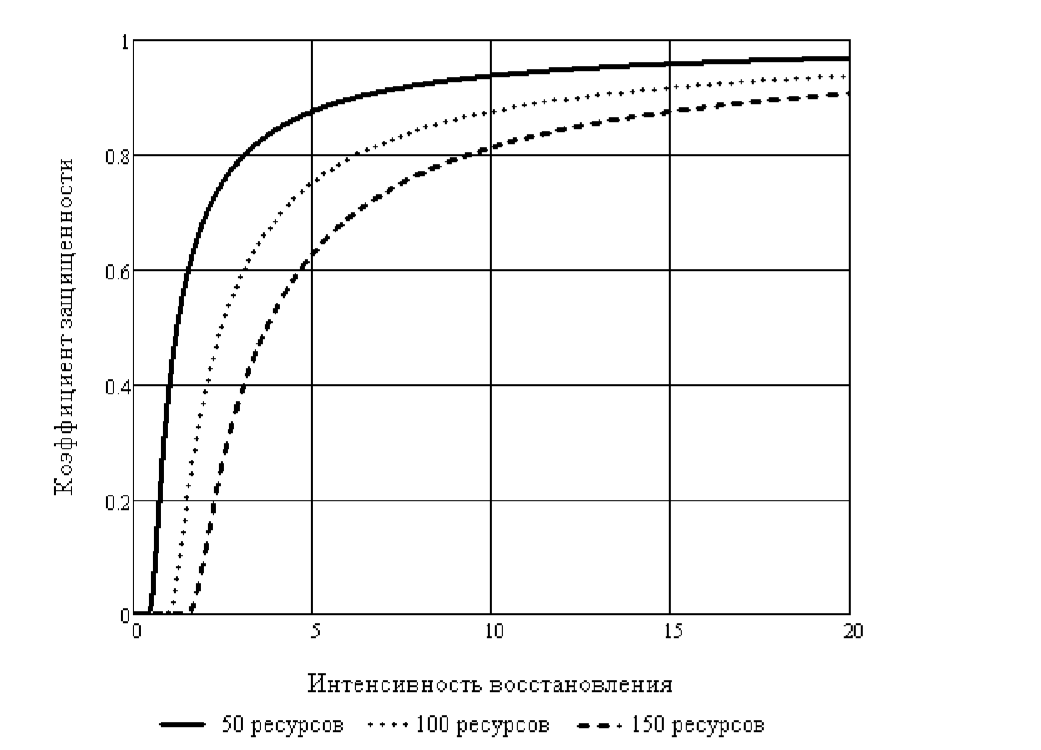


Рис. . Залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення захищеності ресурсів при обмежених ресурсах на відновлення.

Припустимо, що в організації є практично необмежені можливості по відновленню захищеності інформації. Тоді, використовуючи формулу (2), можна отримати залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення захищеності ресурсів (рис. 2).

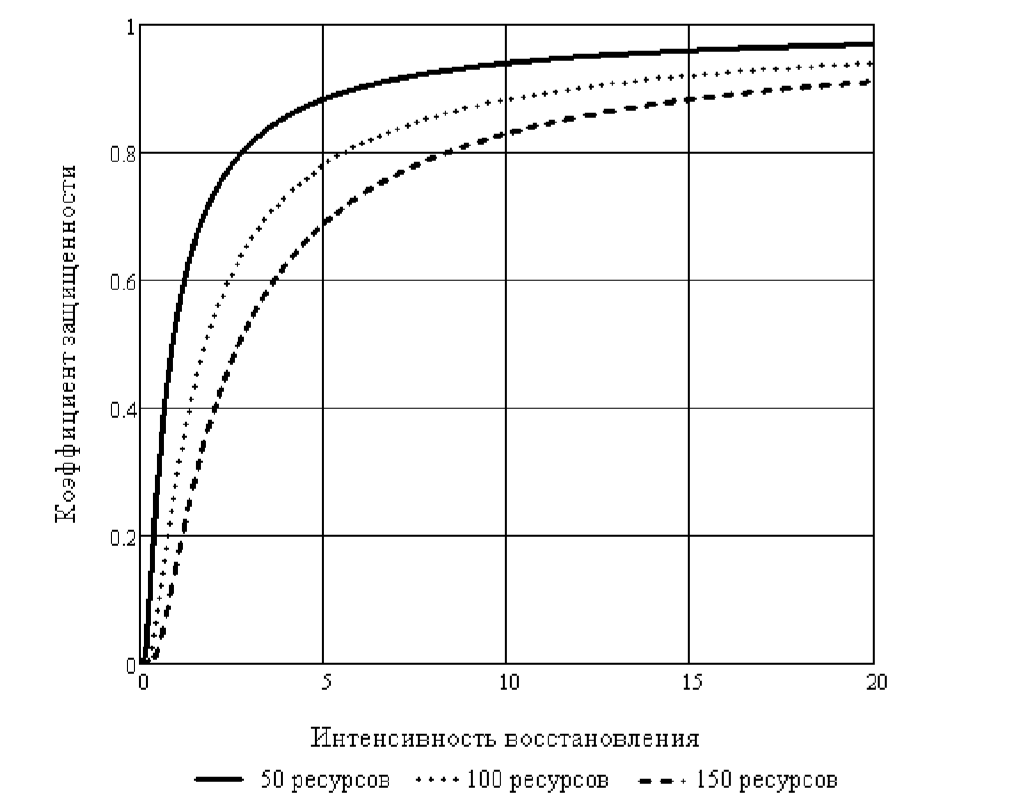


Рис. . Залежність коефіцієнта захищеності інформації в АС від інтенсивності відновлення захищеності ресурсів при умовно необмежених ресурсах на відновлення.

З'ясуємо, яка повинна бути інтенсивність відновлення захищеності ресурсів в АС адміністратором безпеки середнього підприємства (100 захищаються ресурсів) при наступних необхідних значеннях коефіцієнта захищеності інформації від несанкціонованого доступу в АС:

Кзщ1АС = 0.9, Кзщ2АС  = 0.95, Кзщ3АС = 0.99. Так як адміністратор безпеки АС реального підприємства має обмежені ресурси на відновлення захищеності інформації, то для розрахунків буде використовуватися формула (1). Результати розрахунків наведені на рис. 3.

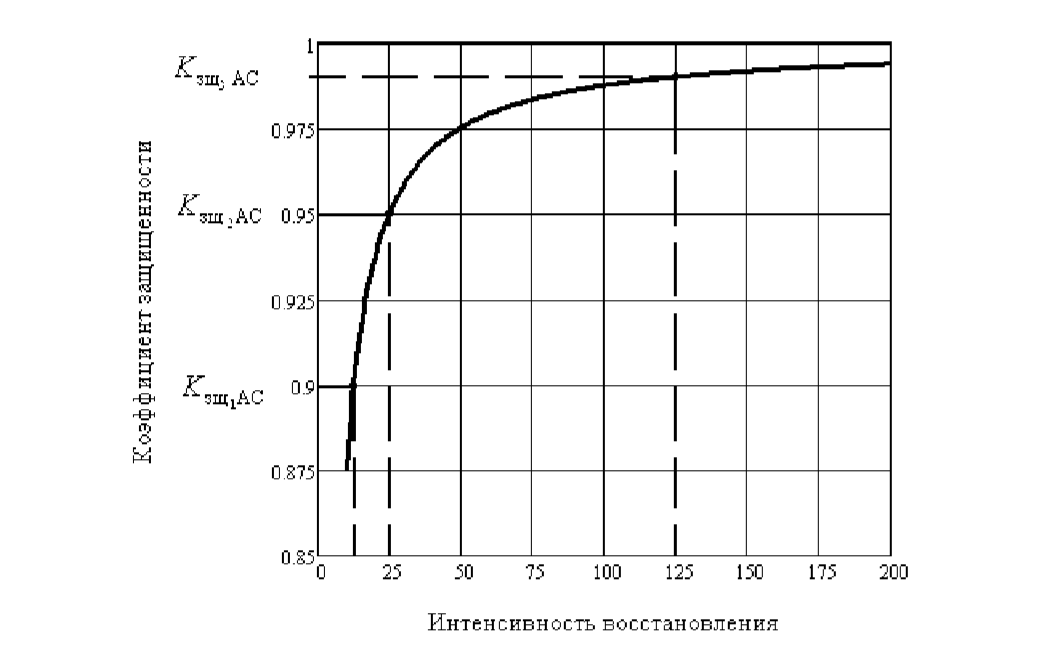


Рис. . Інтенсивність відновлення захищеості ресурсів при Кзщ1АС = 0.9, Кзщ2АС  = 0.95, Кзщ3АС = 0.99

Результати розрахунку часу на відновлення захищеності ресурсів адміністратором безпеки АС представлені в таблиці.

Таблиця

|  |  |  |
| --- | --- | --- |
| КзщАС | µвз, раз / год | Час необхідний на відновлення захищеності ресурсів |
| 0.9 | 12.5 | 4.8 хв |
| 0.95 | 25 | 2.4 хв |
| 0.99 | 125 | 28.8 с |

**Висновки. Контроль захищеності інформації в АС за критерієм придатності дозволяє зробити наступні висновки:**

* Залежність рівня захищеності інформації від несанкціонованого доступу в АС від ресурсів, що виділяються на відновлення захищеності, носить яскраво виражений нелінійний характер. Для кожної АС існує порогове значення виділених ресурсів, перевищення якого практично не призводить до підвищення рівня захищеності.
* Для забезпечення необхідного рівня захищеності необхідно використовувати додаткові і альтернативні засоби захисту.
* Без використання автоматичних засобів виявлення порушень безпеки ресурсів і відновлення захищеності ресурсів АС, здатних функціонувати в масштабі часу, близькому до реального, в умовах експлуатації високий рівень захищеності труднодостіжім.

**АНАЛІЗ ФУНКЦІОНАЛЬНИХ КЛАСІВ**

Аудит безпеки (FAU)

Аудит безпеки включає в себе розпізнавання, запис, збереження та аналіз інформації, пов'язаної з діями, що стосуються безпеки (наприклад, з діями, контрольованими ПБО). Записи аудиту, одержувані в результаті, можуть бути проаналізовані, щоб визначити, які дії, пов'язані з безпекою, відбувалися і хто з користувачів за них відповідає.

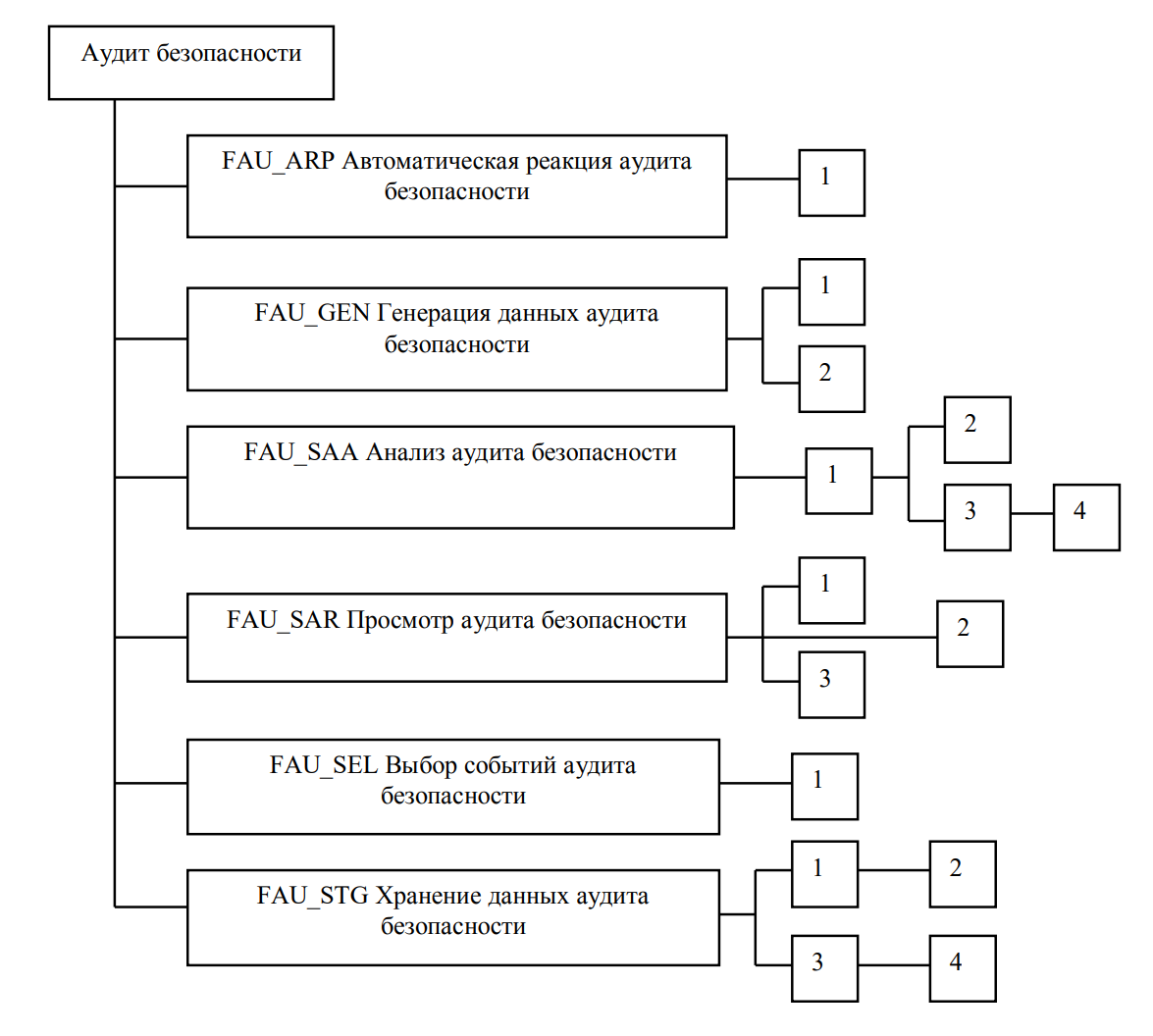


Рис. . Декомпозиція класу «Аудит безпеки»

**Автоматична реакція аудиту безпеки (FAU\_ARP)**

Сімейство FAU\_ARP визначає реакцію на виявлення подій, що вказують на можливе порушення безпеки.

В даному сімействі визначено одну компоненту FAU\_ARP.1 “Сигнали порушення безпеки”. ФБО повинні вживати заходів у разі виявлення можливого порушення безпеки.

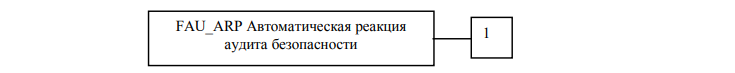


Рис. . Ранжирування компонентів в FAU\_ARP

**Генерація даних аудиту безпеки (FAU\_GEN)**

Сімейство FAU\_GEN визначає вимоги щодо реєстрації виникнення подій, що відносяться до безпеки, які підконтрольні ФБО. Це сімейство ідентифікує рівень аудиту, перераховує типи подій, які потенційно повинні піддаватися аудиту з використанням ФБО, і визначає мінімальний обсяг пов'язаної з аудитом інформації, яку слід подавати в записах аудиту різного типу.



Рис. . Ранжирування компонентів в FAU\_ GEN

В **FAU\_GEN** визначено наступні компоненти:

* FAU\_GEN.1 «Генерація даних аудиту»
* FAU\_GEN.2 «Асоціація ідентифікатора користувача»

FAU\_GEN.1 визначає рівень подій, потенційно піддаються аудиту, і склад даних, які повинні бути зареєстровані в кожному записі.

Згідно до FAU\_GEN.2 ФБО повинні асоціювати події, які потенційно піддаються аудиту, і особисті ідентифікатори користувачів.

**Аналіз аудиту безпеки (FAU\_SAA)**

Сімейство FAU\_SAA визначає вимоги до автоматичних засобів, які аналізують показники функціонування системи і дані аудиту з метою пошуку можливих або реальних порушень безпеки. Цей аналіз може використовуватися для підтримки як виявлення втручання, так і автоматичного реагування на очікуване порушення безпеки.

Дії, що вживаються при виявленні порушень, можуть бути при необхідності визначені з використанням сімейства FAU\_ARP.

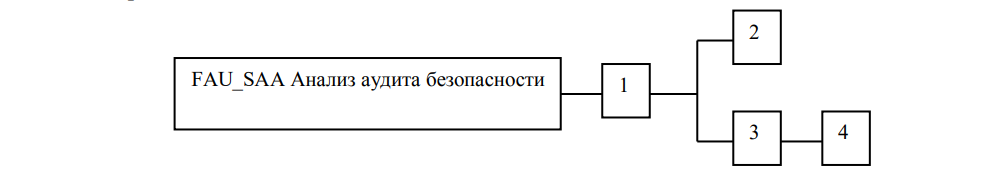


Рис. . Ранжирування компонентів в FAU\_ARP

Компонента FAU\_SAA.1 «Аналіз потенційного порушення» визначає поріг виявлення на основі раніше визначеного набору правил.

У відповідності до FAU\_SAA.2 «Виявлення аномалії, засноване на профілі» ФБО підтримують окремі профілі використання системи, де профіль являє собою шаблони передісторії використання, що виконувалися учасниками цільової групи профілю. Цільова група профілю може включати в себе одного або декількох учасників, які взаємодіють з ФБО. Кожному учаснику цільової групи профілю призначається індивідуальний рейтинг підозрілої активності, який показує, наскільки поточні показники дій учасника відповідають встановленим шаблонами використання, представленим в профілі. Цей аналіз може виконуватися під час функціонування ГО або при аналізі даних аудиту в пакетному режимі.

Згідно до FAU\_SAA.3 «Проста евристика атаки» ФБО повинні бути здатні виявити виникнення характерних подій, які свідчать про значну загрозу здійсненню ПБО. Цей пошук характерних подій може відбуватися в режимі реального часу або при аналізі даних аудиту в пакетному режимі.

FAU\_SAA.4 «Складна евристика атаки» стверджує, що ФБО повинні бути здатні визначити і виявити багатокрокові сценарії проникнення. Тут ФБО здатні порівняти події в системі (можливо, що виконуються декількома учасниками) з послідовностями подій, відомими як повні сценарії проникнення. ФБО повинні бути здатні вказати на виявлення характерного події або послідовності подій, які свідчать про можливе порушення ПБО.

**Перегляд аудита безпеки (FAU\_SAR)**

Це сімейство визначає вимоги до інструментів аудиту, які повинні бути доступними авторизованим користувачам для надання допомоги у перегляді даних аудиту.

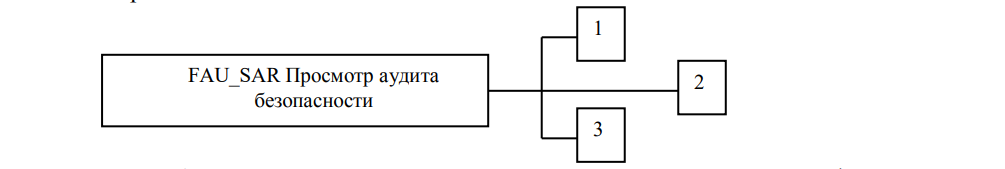


Рис. . Ранжирування компонентів в **FAU\_SAR**

FAU\_SAR.1 Аудиторський огляд забезпечує можливість читання інформації з аудиторських записів.

FAU\_SAR.2 Обмежений аудит вимагає, щоб не було інших користувачів, крім тих, що були ідентифіковані в FAU\_SAR.1, які можуть читати інформацію.

FAU\_SAR.3. Вибір аудиторського розгляду вимагає інструментів перевірки аудиту, щоб вибрати дані аудиту, які будуть переглянуті на основі критеріїв.

**Вибір події з аудиту безпеки (FAU\_SEL)**

Це сімейство визначає вимоги до вибору події, яка повинна бути перевірена під час роботи ОО. Він визначає вимоги до включення або виключення подій із сукупності аудиторських подій.

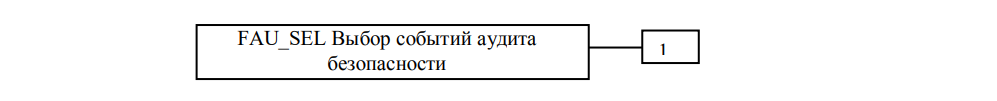


Рис. . Ранжирування компонентів в **FAU\_SEL**

FAU\_SEL.1 “Вибірковий аудит” вимагає можливості включати чи виключати події з набору подій, що перевіряються, згідно до атрибутів, що визначаються автором ПЗ / ЗБ.

**Зберігання даних, які отримані за результатами аудиту безпеки (FAU\_STG)**

Це сімейство визначає вимоги до ФБО, для отримання можливості створювати та підтримувати безпечну історію проведення аудиту.

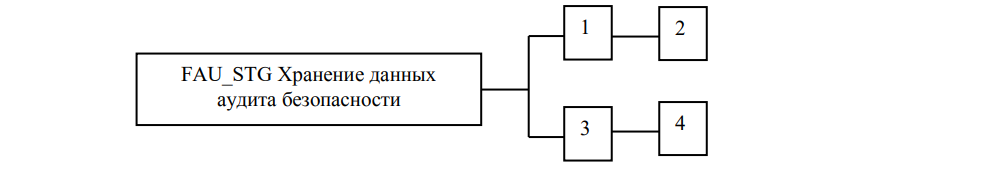


Рис. . Ранжирування компонентів в **FAU\_STG**

Відповідно до FAU\_STG.1 “Захищені сховища журналів аудиту” журнали мають розміщуються так, аби вони були захищеними від несанкціонованого видалення та / або модифікації.

FAU\_STG.2 “Гарантії доступності даних аудиту” вказує на те, що ФБО підтримує дані аудиту з урахуванням виникнення небажаного стану.

FAU\_STG.3 “Дії у разі вірогідної втрати даних аудиту” описує дії, які слід вжити, якщо перевищено порогове значення наповнення журналу аудиту.

FAU\_STG.4 “Попередження втрати даних аудиту” вказує на те, як слід чинити у разі переповнення журналу аудиту.

**Зв’язок (FCO)**

Цей клас включає два сімейства, які специфічно пов'язані з забезпеченням ідентичності сторони, яка бере участь у обміні даними. Ці сімейства пов'язані з забезпеченням ідентичності джерела переданої інформації (підтвердження походження) та забезпечення ідентифікації одержувача переданої інформації (підтвердження отримання). Ці сімейства гарантують, що автор не може заперечувати факт надсилання повідомлення, а одержувач не зможе заперечити, що отримав це повідомлення.



Рис. . Декомпозиція класу “Зв’язок”

В класі визначено два сімейства:

* Невідхильність надсилання (FCO\_NRO)
* Невідхильність отримування (FCO\_NRR)

**Невідхильність** надсилання **(FCO\_NRO)**

Неможливість відмови від відправлення гарантує, що джерело інформації не зможе успішно відмовити у надсиланні інформації. Це сімейство вимагає, щоб ФБО забезпечували методи, які гарантували б, що суб'єкт, який отримує інформацію під час обміну даними, має докази походження інформації.

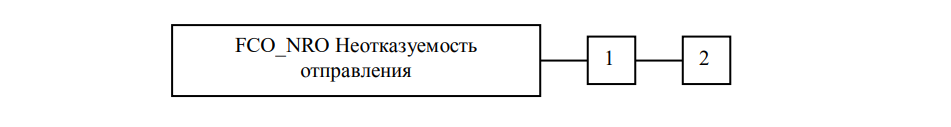


Рис. . Ранжирування компонентів в **FCO\_NRO**

FCO\_NRO.1 “Вибіркове підтвердження походження” вимагає від ФБО надання суб'єктам можливості запитувати докази походження інформації.

FCO\_NRO.2 “Примусовий доказ походження” вимагає, щоб ФБО завжди генерували докази походження для переданої інформації.

Невідхильність отримування (FCO\_NRR)

Неможливість відмови від отримання гарантує, що одержувач інформації не зможе успішно відмовити в отриманні інформації. Це сімейство вимагає, щоб ФБО надавали методи, для гарантування того, що суб'єкт, який передає інформацію під час обміну даними, має докази отримання інформації.

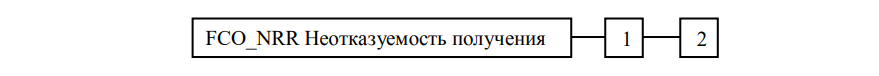


Рис. . Ранжирування компонентів в **FCO\_NRR**

FCO\_NRR.1 “Вибіркове підтвердження отримання” вимагає, щоб ФБО надавали суб'єктам здатність подавати докази про отримання інформації.

FCO\_NRR.2 “Примусове підтвердження отримання” вимагає, щоб ФБО завжди надавали докази отримання для отриманої інформації

**Ідентифікація та аутентифікації (FIA\_AFL)**

Сімейства цього класу відповідають вимогам щодо функцій для встановлення та підтвердження заявленої ідентифікації користувача.

Ідентифікація та автентифікація необхідні для забезпечення відповідності користувача відповідним атрибутам безпеки (наприклад, ідентифікація, групи, ролі, рівні безпеки та цілісності).

Неодмінна ідентифікація авторизованих користувачів та правильне об'єднання атрибутів безпеки з користувачами та темами має вирішальне значення для забезпечення виконання передбачених правил безпеки.

Сім'ї в цьому класі займаються визначенням та перевіркою ідентичності користувачів, визначенням їх повноважень для взаємодії з ФБО та правильною асоціацією атрибутів безпеки для кожного авторизованого користувача. Інші категорії вимог (наприклад, захист даних користувачів, аудит безпеки) залежать від правильної ідентифікації та автентифікації користувачів, щоб вони були ефективними.

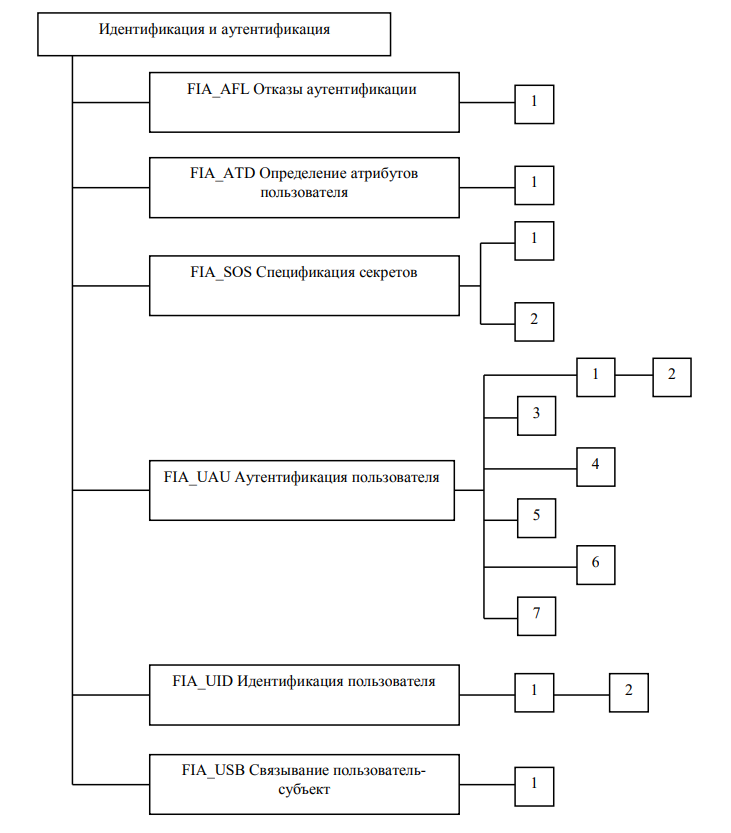


Рис. . Декомпозиція класу FIA

**Відмови в аутентифікації (FIA\_AFL)**

Це сімейство містить вимоги до визначення значень кількості невдалих спроб автентифікації та дій ФБО у випадках невдалих спроб автентифікації. Параметри включають (але не обмежуються) кількість невдалих спроб аутентифікації та порогові значення часу.

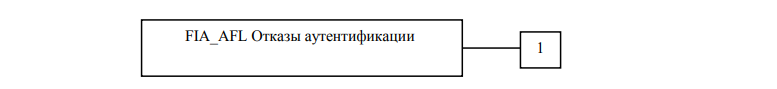


Рис. . Ранжирування компонентів в **FIA\_AFL**

FIA\_AFL.1 “Обробка відмов аутентифікації” вимагає, щоб ФБО мали змогу припинити процес встановлення сесії після певної кількості невдалих спроб автентифікації користувача. Також вимагається, щоб після закінчення процесу встановлення сесії ФБО могли відключити обліковий запис користувача або точку входу (наприклад, робоча станція), з якої були зроблені спроби, поки адміністратор не прийме відповідне рішення.

**Визначення атрибутів для користувачів (FIA\_ATD)**

Всі авторизовані користувачі можуть мати набір атрибутів безпеки, окрім ідентифікатора користувача, який використовується для забезпечення виконання ПБО. Це сімейство визначає вимоги щодо асоціації атрибутів захисту із користувачами, якщо це необхідно для підтримки ПБО.

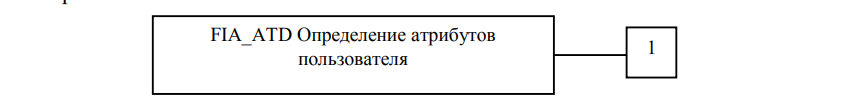


Рис. . Ранжирування компонентів в **FIA\_ATD**

FIA\_ATD.1 “Визначення атрибута користувача”, дозволяє зберігати атрибути безпеки для кожного користувача індивідуально.

**Специфікація секретів (FIA\_SOS)**

Це сімейство визначає вимоги до механізмів, що забезпечують встановлені показники якості на наданих секретах та створюють секрети для задоволення визначеної метрики.

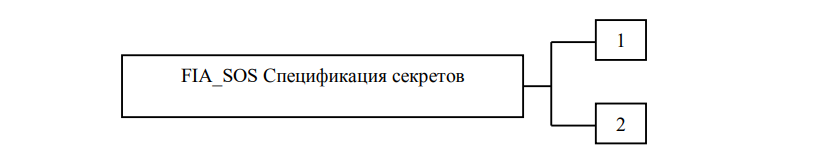


Рис. . Ранжирування компонентів в **FIA\_SOS**

FIA\_SOS.1 “Перевірка секретності” вимагає, щоб ФБО перевірила, чи секрети відповідають визначеним показникам якості.

FIA\_SOS.2 “Створення секретів” вимагає від ФБО генерувати секрети, які відповідають певним показникам якості.

**Аутентифікація користувача (FIA\_UAU)**

Це сімейство визначає типи механізмів автентифікації користувачів, які підтримуються ФБО. Ця сім'я також визначає необхідні атрибути, на яких повинні базуватися механізми автентифікації користувача.



Рис. . Ранжирування компонентів в **FIA\_UAU**

FIA\_UAU.1 “Терміни автентифікації”, дозволяють користувачеві виконувати певні дії до автентифікації користувача.

FIA\_UAU.2 “Аутентифікація користувача перед будь-якою дією користувача“ вимагає, щоб користувачі самостійно автентифікувались, перш ніж вчинити дію ФБО дасть їм можливість виконвати якісь дії.

FIA\_UAU.3 “Незаперечна автентифікація” вимагає, щоб механізм автентифікації мав можливість виявляти та запобігати використанню підроблених або скопійованих даних аутентифікації.

FIA\_UAU.4 “Механізми одноразового автентифікації”, вимагає механізму автентифікації, який працює з одноразовими даними аутентифікації.

FIA\_UAU.5. “Комбінування механізмів автентифікації” вимагає, щоб для автентифікації ідентифікацій користувачів для певних подій, було надано та використано різні механізми автентифікації.

FIA\_UAU.6 “Повторна автентифікація” вимагається можливість вказати перелік подій, для яких користувачеві потрібно повторно перевірити автентичність.

FIA\_UAU.7 “Автентифікації з захищеним зворотнім зв'язком” вимагає під час автентифікації надання користувачеві обмеженої інформації про неї.

**Ідентифікація користувача (FIA\_UID)**

Це сімейство визначає умови, за яких користувачі повинні будуть самостійно ідентифікувати себе перед виконанням будь-яких інших дій, які повинні бути опосередковані ФБО і вимагають ідентифікації користувача.

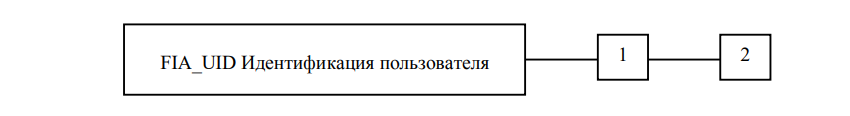


Рис. . Ранжирування компонентів в **FIA\_UID**

FIA\_UID.1 “Терміни ідентифікації” дозволяють користувачам виконувати певні дії, перш ніж вони ідентифікуються за допомогою ФБО.

FIA\_UID.2 “Ідентифікація користувача перед будь-якою дією” вимагає, щоб користувачі ідентифікували себе перед тим, як ФБО дозволять йому виконувати будь-які дії.

**Пов’язування користувач-суб’єкт (FIA\_USB)**

Автентифікований користувач, для того, щоб використовувати ОО, зазвичай активує певний суб’єкт. Атрибути безпеки користувача пов'язуються (повністю або частково) з цим суб’єктом. Це сімейство визначає вимоги щодо створення і підтримки асоціації атрибутів безпеки користувача з суб’єктом, що діє від імені користувача.

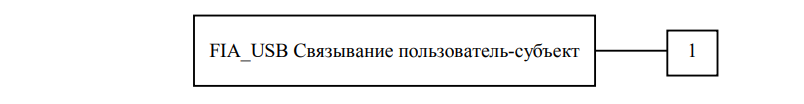


Рис. . Ранжирування компонентів в **FIA\_USB**

FIA\_USB.1 “Зв’язування користувач-суб’єкт” вимагає підтримання зв'язку між атрибутами безпеки користувача та суб'єктом, що діє від імені користувача.

**Приватність (FPR)**

Цей клас містить вимоги щодо конфіденційності. Ці вимоги забезпечують захист користувачів від виявлення та неправильного використання ідентичності іншими користувачами.

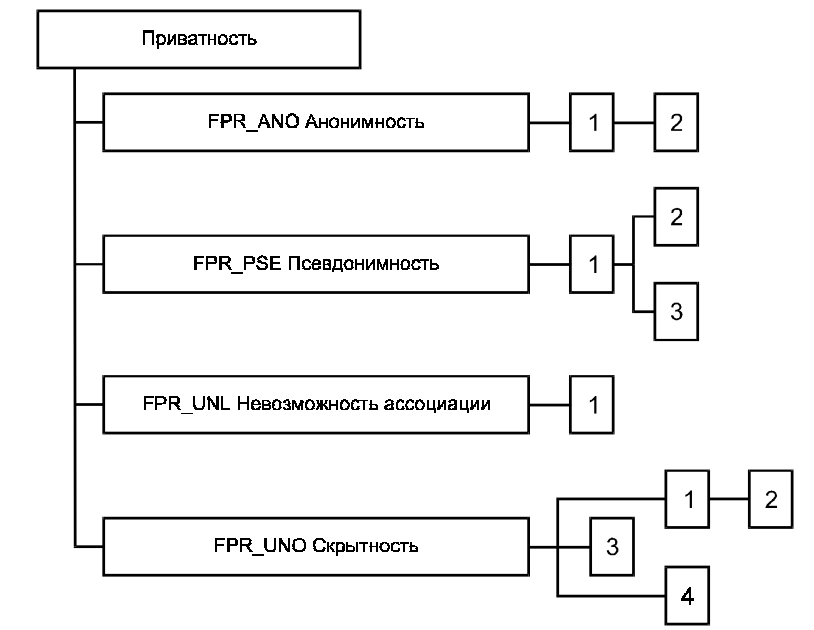


Рис. . Декомпозиція класу **FPR**

**Анонімність (FPR\_ANO)**

Це сімейство гарантує, що користувач може використовувати ресурс чи послугу, не розкриваючи себе. Вимоги до анонімності забезпечують захист ідентичності користувача. Анонімність не покликана захистити предметну ідентичність.



Рис. . Ранжирування компонентів в **FPR\_ANO**

FPR\_ANO.1 “Анонімність” вимагає, щоб будь-який інший користувач або суб’єкт не зміг визначити особу користувача, пов'язаного з предметом або операцією.

FPR\_ANO.2 “Анонімність без запиту інформації” накладає додаткові вимоги на FPR\_ANO.1, забезпечуючи, що ФБО не вимагає ідентифікатор користувача.

**Псевдонімічність (FPR\_PSE)**

Це сімейство гарантує, що користувач може використовувати ресурс чи послугу, не розкриваючи свого ідентифікатора, але все ще може бути відповідальним за виконані дії.



Рис. . Ранжирування компонентів в **FPR\_PSE**

FPR\_PSE.1 “Псевдонімічність” вимагає, щоб набір користувачів та/або суб’єктів не зміг дізнатися ідентифікатор користувача, який пов'язаний з суб'єктом або операцією, але цей користувач все ще ніс відповідальність за виконані дії.

FPR\_PSE.2 “Зворотна псевдонімічність” вимагає від ФБО надавати можливість визначати початковий ідентифікатор користувача на основі наданого псевдоніму.

FPR\_PSE.3 “Альтернативна псевдонімічність” вимагає від ФБО дотримуватися певних правил побудови псевдоніму до ідентифікатора користувача.

**Неможливість асоціації (FPR\_UNL)**

Це сімейство гарантує, що користувач може багаторазово використовувати ресурси чи послуги, при цьому інші користувачі не зможуть пов'язувати разом ці спроби.

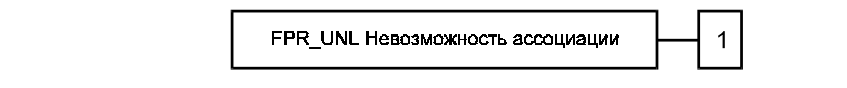


Рис. . Ранжирування компонентів в **FPR\_UNL**

FPR\_UNL.1 “Неможливість асоціаці” вимагає, щоб користувачі та/або суб'єкти не мали змоги визначити, чи викликає один і той самий користувач певні операції в системі.

**Прихованість (FPR\_UNO)**

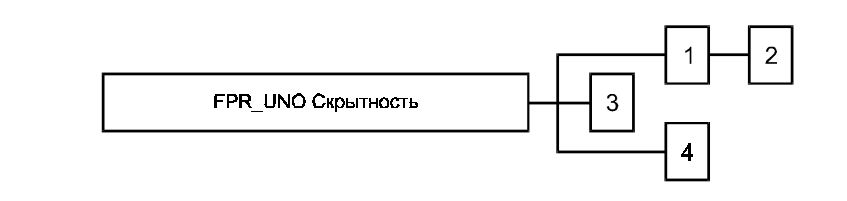


Рис. . Ранжирування компонентів в **FPR\_UNO**

Це сімейство гарантує, що користувач може використовувати ресурс чи послугу без необхідності повідомляти про це інших, особливо третіх сторін.

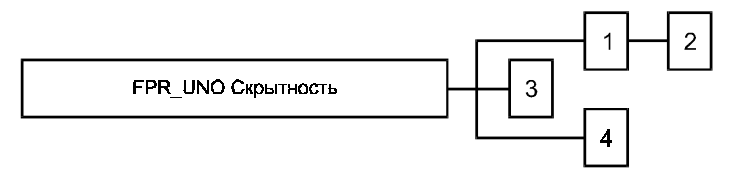


Рис. . Ранжирування компонентів в **FPR\_UNO**

FPR\_UNO.1 “Прихованість” вимагає, щоб користувачі та/або суб'єкти не мали змоги визначити, чи виконується операція.

FPR\_UNO.2. “Розподіл інформації, що впливає на прихованість”, вимагає, щоб в ФБО були передбачені спеціальні механізми, що дозволяють уникнути концентрації інформації, пов'язаної з конфіденційністю, в межах ОО. Такі концентрації можуть вплинути на прихованість, якщо виникне порушення безпеки.

FPR\_UNO.3 “Прихованість без запиту інформації” вимагає, щоб ФБО не намагалися отримати конфіденційну інформацію, яка зможе бути використаною для порушення прихованості.

FPR\_UNO.4. “Відкритісь для уповноваженого користувача”. Для одного чи декількох таких користувачів ФБО повинні забезпечити здатність спостерігати за використанням ресурсів та/або послуг.

**Доступ до ОО (FTA)**

Це сімейство визначає функціональні вимоги для контролю за встановленням сеансів користувачів.

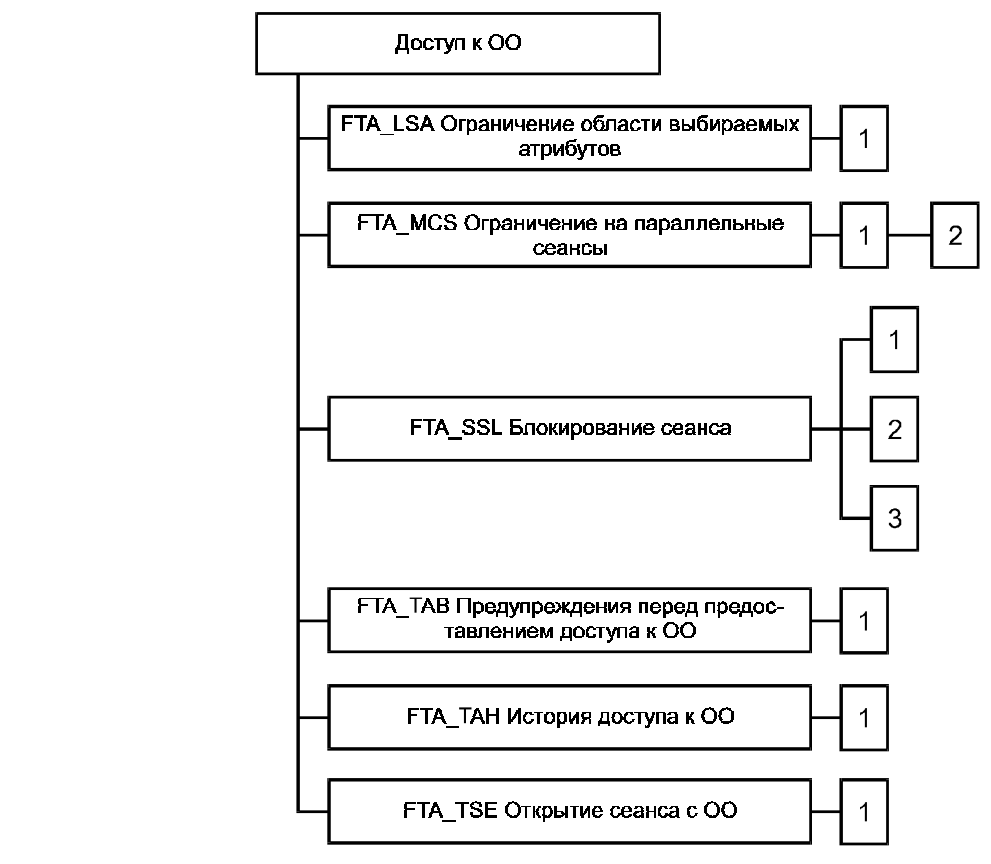


Рис. . Декомпозиція класу **FTA**

**Обмеження обсягу виділених атрибутів (FTA\_LSA)**

Це сімейство визначає вимоги до обмеження обсягу атрибутів безпеки сеансу, які можуть бути вибраними користувачем для даного сеансу.

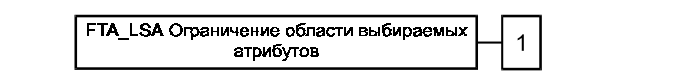


Рис. . Ранжирування компонентів в **FPR\_UNO**

**Криптографічна підтримка (FCS)**

ФБО може використовувати криптографічні функції, щоб задовольнити декілька цілей безпеки високого рівня. До таких цілей можна віднести: ідентифікацію та автентифікацію, неповторність, довірений шлях, довірений канал та розділення даних. Цей клас використовується, коли ОО реалізує криптографічні функції, реалізація яких може здійснюватися в апаратно-програмними та/або програмними методами.

Клас FCS складається з двох сімейств: FCS\_CKM – “управління криптографічними ключами” та “криптографічні операції” FCS\_COP. Перше розглядає аспекти керування криптографічними ключами, тоді як FCS\_COP стосується оперативного використання цих криптографічних ключів.

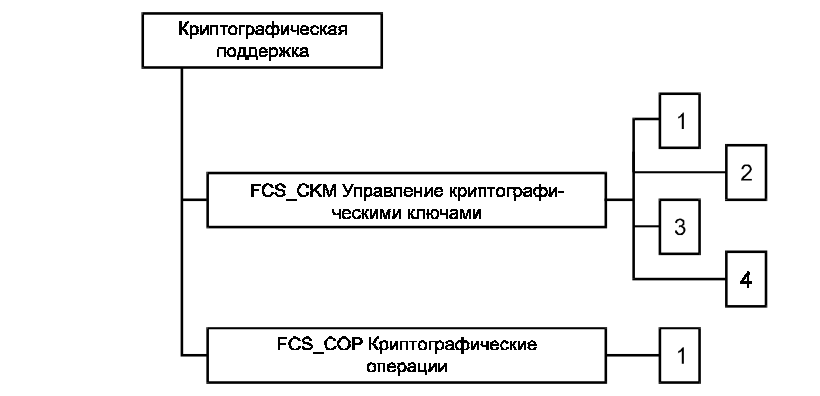


Рис. . Декомпозиція класу **FCS**

**Управління криптографічними ключами (FCS\_CKM)**

Управління криптографічними ключами повинно відбуватись протягом всього їх життєвого циклу. Це сімейство призначене для підтримки цього життєвого циклу і, отже, визначає вимоги до таких дій: генерація, розповсюдження, доступ та знищення криптографічного ключа. Це сімейство повинне бути включеним, коли є функціональні вимоги до управління криптографічними ключами.



Рис. . Ранжирування компонентів в **FCS\_CKM**

FCS\_CKM.1 “Створення криптографічного ключа” вимагає створювати криптографічні ключі у відповідності до заданого алгоритму та розмірів ключів, які базуються на відповідному стандарті.

FCS\_CKM.2 “Розповсюдження криптографічного ключа” вимагає щоб криптографічні ключі розповсюджувались у відповідності до заданого методу розподілу, який базується на відповідному стандарті.

FCS\_CKM.3 “Доступ до криптографічного ключа” вимагає щоб доступ до ключів відбувався у відповідності до заданого методу доступу, який базується на певному стандарті.

FCS\_CKM.4 “Деструкція криптографічного ключа” вимагає знищення криптографічних ключів у відповідності до заданого методу знищення, який базується на певному стандарті.

**Криптографічні операції (FCS\_COP)**

Для правильної роботи криптографічної операції операція повинна виконуватися у відповідності з заданим алгоритмом та криптографічним ключем заданого розміру. Це сімейство має бути включеним, коли існують вимоги щодо виконання таких операцій.

Типові криптографічні операції включають в себе шифрування та/або дешифрування даних, створення та/або перевірку цифрових підписів, генерацію криптографічної контрольної суми для цілісності та/або перевірки контрольної суми, безпечного хешування, шифрування та/або дешифрування ключа та угоду про криптографічні ключі .



Ранжирування компонентів в **FCS\_COP**

FCS\_COP.1 “Криптографічні операції” вимагає виконання криптографічної операції у відповідності до заданого алгоритму та ключа з заданими розмірами. Вказаний алгоритм та розміри ключа взмозі базуватися на певному стандарті.

**Довірені шляхи та канали (FTP)**

Сімейства цього класу встановлюють вимоги до надійного шляху зв'язку між користувачами та ФБО, а також до надійного каналу зв'язку між ФБО та іншими довіреним ІТ-продуктами. Довірені маршрути та канали можна охарактеризувати наступним чином:

* Маршрут будується за допомогою внутрішніх та зовнішніх каналів зв'язку (відповідно до компоненту), які ізолюють ідентифіковану підмножину даних та команд ФБО від інших частин ФБО та даних користувача.
* Використання маршруту може ініціювати користувач та/або ФБО (відповідно до компоненту)
* Маршрут здатний забезпечити впевненість, що користувач обмінюється даними з правильними ФБО, і що ФБО виконує обмін з правильним користувачем (відповідно до компонента)

У цій парадигмі довіреним каналом є канал зв'язку, який може ініціювати будь-яка зі сторін каналу, що зв’язуються, і забезпечує неможливість відмови від ідентичності сторін каналу.

Довірений маршрут забезпечує можливості для користувачів виконувати функції прямо взаємодіючи з ФБО. Довірений шлях, як правило, бажаний для дій користувача, таких як початкова ідентифікація та/або автентифікація, але може також бути використаним і під час всього сеансу. Обміни по довіреному маршруту можуть ініціюватися користувачем або ФБО. Довірений маршрут гарантує, що відповіді, отримані за його допомогою захищаються від модифікації або розголошення ненадійними програмами.

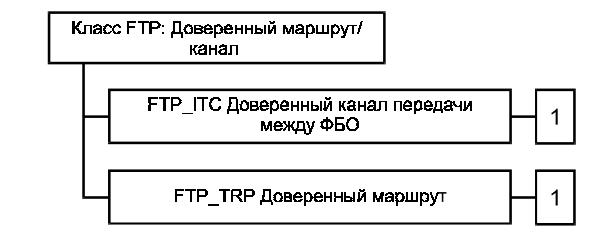
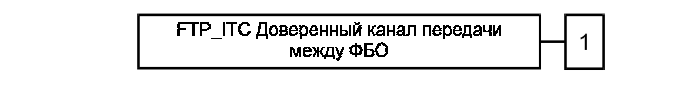


Рис. . Декомпозиція класу **FTP**

**Надійний канал передачі між ФБО (FTP\_ITC)**

Це сімейство визначає вимоги до створення надійного каналу між ФБО та іншими надійними ІТ-продуктами для виконання операцій, які критичні для безпеки. Дане сімейство слід включати, коли існують вимоги до безпечної передачі даних користувача або ФБО між ОО та іншими надійними ІТ-продуктами.

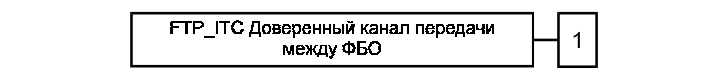


Ранжирування компонентів в **FTP\_ITC**

FTP\_ITC.1 “Довірений канал між ФБО“ вимагає, щоб ФБО забезпечували довірений канал зв'язку між собою та іншим надійними ІТ-продуктоми.

**Довірений маршрут (FTP\_TRP)**

Це сімейство визначає вимоги щодо встановлення та підтримки довірених комунікацій між користувачами та ФБО. Довірений шлях може знадобитися для будь-якої взаємодії, що стосується безпеки. Обмін надійними шляхами може бути ініційований користувачем під час взаємодії з ФБО, або ФБО можуть встановити зв'язок з користувачем через довірений шлях.



Ранжирування компонентів в **FTP\_TRP**

FTP\_TRP.1 “Довірені маршрути” вимагає, щоб надійний маршрут між ФБО і користувачем був забезпечений для набору подій, визначених автором ПЗ/ЗБ. Користувач та/або ФБО можуть мати можливість ініціювати довірений маршрут.