УДК 004.681:681.3.06

Тіскіна О.О. (ДУІКТ)
Чередниченко В.С. (ДУІКТ)

ВИМОГИ ДО СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Для розгляду проблеми захисту інформації (ЗІ) в загальному вигляді виділимо в її предметній області три наступні ієрархії: структурну, причинно-наслідкову і функціональну [1].

Способи ЗІ залежать від типу інформації, форми її зберігання, обробки і передачі, типу носія інформації, а також передбачуваного способу нападу і наслідків його впливу на інформацію.

В основному власник інформації не знає де, коли і яким чином буде здійснено напад, тому йому необхідно виявити сам факт нападу. [1,2]

Визначення потенційної цінності інформації дозволяє подумати насамперед про безпеку найбільш важливих секретів, витік яких може завдати збитку. При цьому необхідно встановити [1,2]:

- яка інформація потребує захисту?
- кого вона може цікавити?
- які елементи інформації найбільш цінні?
- який «термін життя» цих секретів?
- у що обійдеться захист інформації?

Досвід застосування систем ЗІ (СЗІ) показує [2], що ефективною може бути лише комплексна система захисту інформації (КСЗІ), яка поєднує наступні заходи: законодавчі, морально-етичні, фізичні, адміністративні, технічні, криптографічні, програмні.

Обгрунтований вибір необхідного рівня захисту інформації є системоутворюючим завданням, оскільки як заниження, так і завищення рівня неминуче веде до втрат. При цьому останнім часом роль даного питання різко зросла у зв'язку з тим, що, по-перше, тепер у число захищуваних окрім військових, державних і відомчих, включені також секрети промислові, комерційні і навіть особистісні, а по-друге, сама інформація все частіше стає товаром.

Основна частина

Вимоги щодо ЗІ визначаються власником інформації, і узгоджуються з виконавцем робіт з проектування і створення СЗІ.

Відповідно до ДСТУ 3396.0-96 і ДСТУ 3396.1-96 визначені основні положення і порядок проведення робіт зі створення СЗІ. Ці стандарти встановлюють об'єкт захисту, мету, основні організаційно-технічні положення СЗІ, неправомірний доступ до якої може завдати збитку громадянам, організаціям, державі, а також категорії нормативних документів з СЗІ і вимоги до порядку проведення робіт з технічного захисту.

Виходячи з цих документів, метою СЗІ є запобігання витоку або порушенню цілісності інформації з обмеженим доступом (Із ОД).

Мета КСЗІ може бути досягнута побудовою СЗІ, яка є організованою сукупністю методів і засобів забезпечення СЗІ.

Технічний захист інформації (ТЗІ) здійснюється поетапно:

1 етап – визначення і аналіз загроз;

2 етап – розробка СЗІ;

3 етап – реалізація плану ЗІ;

4 етап – контроль функціонування і управління СЗІ.

Зміст і послідовність робіт з протидії загрозам або їх нейтралізації повинні відповідати вказаним в ДСТУ 3396.0-96 етапам функціонування системи захисту інформації, відповідно до ДСТУ 3396.1-96, і полягати в:

–проведенні обстеження об'єкту (підприємства, установи, організації);

–розробці і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;

–прийому робіт з ТЗІ;

–атестації засобів (систем) забезпечення інформаційної діяльності на відповідність вимогам нормативних документів системи ТЗІ.

У процесі формування вимог до СЗІ доцільно знайти відповіді на наступні питання:

–які заходи безпеки пропонується використовувати?

–яка вартість доступних програмних і технічних заходів захисту?

–наскільки ефективні доступні заходи захисту?

–наскільки уразливі підсистеми СЗІ?

–чи є можливість провести аналіз ризику?

Сукупність вимог до СЗІ наведено на рис. 1.

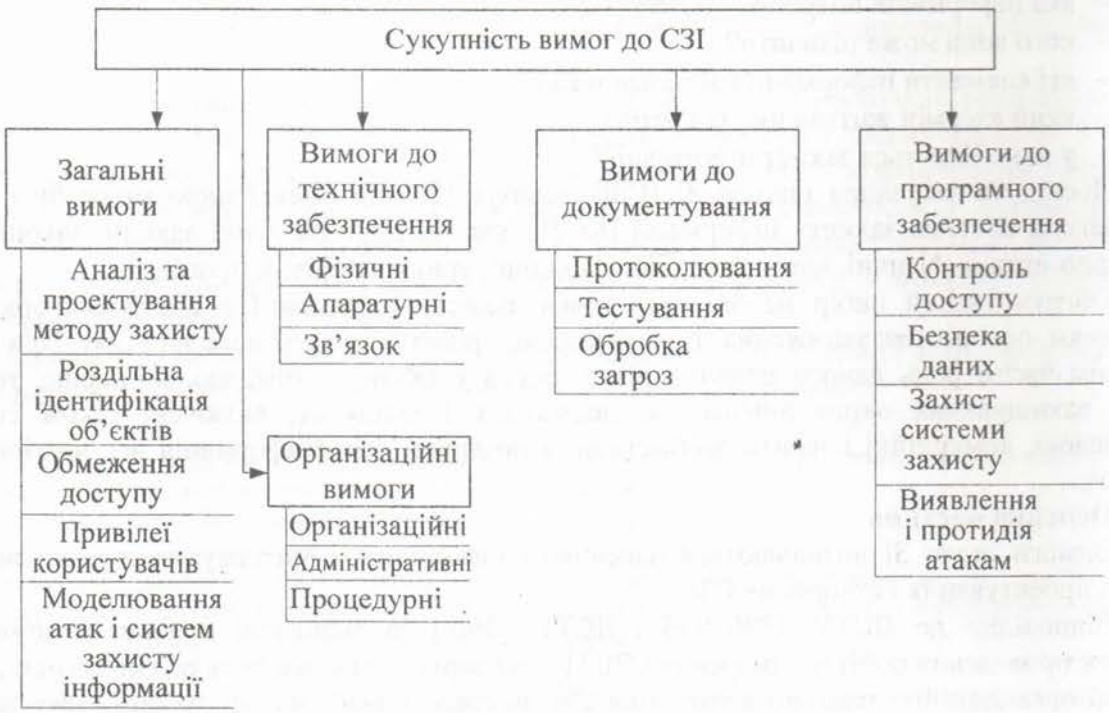

Рис. 1 Сукупність вимог до СЗІ

У загальному випадку доцільно виділити наступні групи вимог до СЗІ:

–загальні вимоги;

–організаційні вимоги;

–конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів, методів і засобів захисту.

Слід зазначити, що в [3] описані тільки вимоги до СЗІ та об'єктів обчислювальної техніки. У [4,5] представлені вимоги і порядок проведення робіт по розробці та введення в експлуатацію систем захисту на об'єктах різного призначення. Тому використовуючи положення приведені в [2,3,4,5] проведемо розробку і сформулюємо вимоги до систем ЗІ для

широкого класу систем і об'єктів. Крім того розгянемо і врахуємо в цих вимогах вплив зовнішніх атак і дій зловмисників, що відсутній в літературі.

Загальні вимоги. Перш за все, необхідна повна ідентифікація користувачів, терміналів, програм, а також основних процесів і процедур, що відбуваються на об'єкті захисту. Крім того, слід обмежити доступ до інформації, використовуючи сукупність наступних способів:

–ієрархічна класифікація доступу;

–класифікація інформації за важливістю і місцем її виникнення;

–вказівки обмежень до інформаційних об'єктів;

–визначення програм і процедур, наданих тільки конкретним користувачам.

СЗІ повинна гарантувати, що будь-який рух інформації ідентифікується, авторизується, виявляється і документується.

Зазвичай формулюються загальні вимоги до СЗІ, які відповідають наступним характеристикам:

–способам побудови СЗІ або її окремих компонентів;

–архітектурі засобів обчислювальної техніки та інформаційних систем (до класу і мінімальної конфігурації ЕОМ, операційного середовища, орієнтації на ту або іншу програмну і апаратну (технічну) платформи);

–застосуванню стратегії захисту;

–витратам ресурсів на забезпечення СЗІ;

–надійності і живучості функціонування СЗІ;

–кількості ступенів секретності інформації, підтримуваних СЗІ;

–забезпеченню швидкості обміну інформацією на об'єкті, у тому числі з урахуванням використовуваних криптографічних вимог;

–кількості підтримуваних СЗІ рівнів повноважень;

–можливості СЗІ обслуговувати певну кількість користувачів;

–тривалість процедури генерації програмної версії СЗІ;

–тривалість процедури підготовки СЗІ до роботи після подачі живлення на компоненти об'єкту;

–можливість СЗІ реагувати на спроби несанкціонованого доступу або атаки ззовні;

–наявності і забезпеченню автоматизованого робочого місця адміністратора ЗІ;

–складу використовуваного програмного і лінгвістичного забезпечення, до його сумісності з іншими програмними платформами, до можливості модифікації і т.п.;

–використовуваним компонентам СЗІ, що купуються (наявність ліцензії, сертифіката і тому подібне).

Організаційні вимоги до системи захисту передбачають реалізацію сукупності адміністративних і процедурних заходів.

Вимоги із забезпечення збереження повинні виконуватися перш за все на адміністративному рівні. Організаційні заходи, що проводяться з метою підвищення ефективності ЗІ, повинні передбачати наступні процедури:

–обмеження несупроводжуваного доступу до інформації;

–здійснення контролю за зміною в системі програмного забезпечення;

–виконання тестування і верифікація змін у системі програмного забезпечення і програмах захисту;

–організацію і підтримку взаємного контролю за виконанням правил захисту інформації;

–обмеження привілеїв персоналу, що обслуговує СЗІ;

–здійснення запису протоколу про доступ до системи;

–гарантію компетентності обслуговуючого персоналу;

–розробку послідовного підходу до забезпечення збереження інформації для об'єкту, що захищається;

–організацію чіткої роботи бібліотеки;

–комплектування основного персоналу на базі інтегральних оцінок і твердих знань;

–організацію системи навчання і підвищення кваліфікації обслуговуючого персоналу.

З погляду забезпечення доступу до інформації, що захищається, необхідно виконати наступні процедурні заходи:

–розробити і затвердити інструкції на завантаження і зупинку роботи операційної системи;

–контролювати використання магнітних носіїв і лістингів, порядок зміни програмного забезпечення і доведення цих змін до користувача;

–розробити процедуру відновлення системи при відмовах;

–встановити політику обмежень і визначити обсяг інформації, що видається;

–розробити систему протоколювання використання ЕОМ СЗІ, введення інформації і виведення результатів;

–забезпечити проведення періодичного чищення архівів для видалення і ліквідації не потрібної і застарілої інформації;

–підтримувати документацію СЗІ відповідно до встановлених правил і стандартів.

Вимоги до підсистем ЗІ в загальному випадку доцільно умовно розділити:

–підсистема управління доступу до інформації (включає також функції управління СЗІ в цілому);

–підсистема реєстрації та обліку дій користувачів (процесів);

–криптографічну підсистему;

–підсистему забезпечення цілісності інформаційних ресурсів та їх конфігурацій.

Для кожної з підсистеми визначаються вимоги у вигляді:

–переліку забезпечуваних підсистемою функцій захисту;

–основних характеристик цих функцій;

–переліку засобів, що реалізують ці функції.

Підсистема управління доступом повинна забезпечувати:

–ідентифікацію, аутентифікацію і контроль за доступом користувачів до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроїв, програм, каталогів, файлів і т.д.;

–очищення областей оперативної пам'яті і зовнішніх накопичувачів системи, що звільняються.

Підсистема реєстрації та обліку виконує:

–реєстрацію та облік доступу до ресурсів системи, видачі вихідних документів, запуску програм і процесів, доступу до файлів, що захищаються, передачу інформації по лініях і каналах зв'язку;

–реєстрацію зміни повноважень доступу, створення об'єктів доступу, що підлягають захисту;

–облік носіїв інформації;

–сповіщення про атаки і спроби порушення захисту об'єкту.

Криптографічна підсистема передбачає:

–шифрування конфіденційної інформації;

–шифрування інформації, що належить різним суб'єктам доступу (групам суб'єктів), з використанням різних ключів;

–використання сертифікованих і атестованих криптографічних засобів.

Підсистема забезпечення цілісності повинна здійснювати:

–забезпечення цілісності, програмних засобів і оброблюваної інформації;

–фізичну охорону засобів обробки інформації та її носіїв;

–наявність адміністратора і служби безпеки об'єкту;

–періодичне тестування СЗІ;

–наявність засобів відновлення СЗІ;

–використання сертифікованих засобів захисту;

–контроль за цілісністю: програмних засобів, ЗІ при завантаженні операційного середовища; операційного середовища перед виконанням різних процесів у системі; функціонального програмного забезпечення (ПЗ) та інформації; конфігурації СЗІ і об'єкту захисту;

–оперативне відновлення функцій СЗІ після збоїв;

–тестування засобів захисту інформації;

–виявлення і блокування дій зловмисників;

–контроль доступу до засобів обчислювальної техніки (ЗОТ) СЗІ, що дає упевненість в тому, що тільки авторизований користувач використовує наявні робочі програми та інформацію;

–контроль дій з персональною авторизацією, що забороняє операції, які роблять операційне середовище уразливим;

–захист програмного забезпечення, що виключає пошкодження програм;

–використання тільки ліцензованого продукту з метою забезпечення захисту від вбудованих програмних закладок і програм руйнування інформаційного середовища;

–захист комунікацій для забезпечення захисту інформації, що передається.

Вимоги до технічного забезпечення. У цій групі формуються вимоги до таких параметрів:

–місця застосування засобів захисту;

–способам використання засобів захисту;

–розмірам контрольованої зони;

–необхідній величині показників захищеності, що враховує реальну обстановку на об'єкті;

–застосуванню способів, методів і засобів досягнення заданого рівня захищеності;

–проведенню спецдослідження устаткування і технічних засобів на об'єкті захисту, метою якого є вимір електромагнітних випромінювань і виявлення небезпечних сигналів;

–проведення спецперевірки технічних засобів ЗІ, метою якої є визначення відповідності забезпечення необхідного рівня захищеності об'єкту.

Програмні засоби ЗІ повинні забезпечувати контроль доступу, безпеку інформації і захист самої СЗІ. Для цього необхідно виконати наступні умови:

–об'єкти захисту повинні ідентифікуватися в явному вигляді при використанні паролів і пропусків;

–система контролю доступу має бути достатньо гнучкою для забезпечення багатообразних обмежень і різних наборів об'єктів;

–кожен доступ до захищеного інформативного файлу і пристрою об'єкту або СЗІ повинен прослідживатися через систему контролю доступу для того, щоб фіксувати і документувати будь-яке звернення.

Безпека інформації може забезпечуватися наступною системою заходів:

–інформаційні об'єкти ідентифікуються і забезпечуються інформацією службою безпеки. Доцільно цю інформацію розміщувати не в окремому каталозі, а разом з інформацією, що має мітки;

–кодові слова захисту і паролі розміщуються усередині файлів, що значною мірою підвищує ефективність захисту;

–доступ до інформації доцільний за допомогою непрямих посилань, наприклад, списку користувачів, допущених власником файлу до розміщеної в ньому інформації;

–інформація і програми можуть перетворюватися (кодуватися) внутрішнім способом або архівацією для зберігання.

СЗІ має бути захищена від дії навколишнього середовища. З цією метою виконується наступна сукупність заходів:

–інформація по негативних запитах не видається;

–повторні спроби доступу після невдалих звернень повинні кількісно обмежуватися;

–при зміні конфігурації системи або при її тестуванні функції захисту зберігаються;

–ніякі зміни таблиць безпеки, окрім зміни зі спеціального пристрою або пульта управління, не вирішуються.

У сучасних умовах у процесі взаємодії об'єкта і людини виникають події, процеси або явища, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформації. Проте до теперішнього часу проектували СЗІ і розробляли вимоги до їх здійснюється без урахування відмінних особливостей систем «людина – об'єкт інформації» або «засіб ЗІ – об'єкт інформації».

Для вирішення завдань захисту інформації вводиться множина підрівневого захисту L – кінцева множина елементів l_1, l_2, …, l_k. Кожен підрівень l_i, $1 \le j \le k$, забезпечується застосуванням m_j-го методу захисту об'єкту $W_i \in W$, тобто w_i

$\forall w_i \in W_i l_j(w_i) \sim m_j(w_i)$, $l_j \in L$, $m_j \in M$, $i \in J$, $j=\overline{1,k}$

Потужність множини L збігається з потужністю множини M: $\square L \| = \square M \square$. Сумарний рівень захисту, що забезпечуєтсья сукупністю M (W_i) методів захисту об'єкту має бути не менше базового рівня $J_o(W_i)$ захисту об'єкту W_i:

$$\forall i \in J: J(w_i) = \sum_{j \in J} l_j(w_i) \ge J_o(W_i) \qquad (1)$$

Підсумовування проводиться лише по тих методах, які належать об'єднанню $M(W_i)$, використовуваному для захисту об'єкту W_i.

Вираз (1) і зміст терміну «рівень захисту об'єкта» визначають принципову відмінність завдань захисту об'єкта від завдань створення систем захисту, описаних у [6].

Виходячи зі сказаного, необхідно також оцінити множину вартостей захисту s_1, s_2, ., s_k. Елемент $s_j \in S$, $j=\overline{1,k}$ характеризує величину затрат при реалізації m_j-го методу захисту об'єкту $w_i \in W$ і який забезпечує l_j-й рівень захисту. Потужність множин M, L та S збігаються $M \| = L = S \|$.

Злом системи або порушення системи захисту об'єкту w_i характеризується вірогідністю злому кожного методу захисту і всієї сукупності методів в цілому, сумарною вартістю злому або несанкціоноване проникнення через неї, а також тимчасовими витратами, необхідними для подолання всіх методів, що вживаються для захисту об'єкту w_i. Сумарна вартість несанкціонованих дій, що вживаються для подолання системи захисту має бути більше вартості засобів, що вживаються для захисту об'єкту і самого об'єкту. Тимчасові витрати подолання СЗІ на об'єкті мають бути максимальні, вони, принаймні, мають бути більш ніж для базового обмеження тимчасових витрат нападу системи захисту об'єкту [6,7]. Тільки за цих умов можна вважати за доцільне вибір даної сукупності методів захисту об'єкту і виконання вимог до СЗІ.

Будь-яка атака або несанкціонована дія, що діє на об'єкт, на кожному з тих, що мають у розпорядженні СЗІ засобів захисту відіб'ється по-різному: деякі із засобів можуть бути зруйновані повністю, деякі виведені з ладу частково, а для якихось засобів атака виявиться безпечною. Облік цих відмінностей у результатах дії атаки на засоби захисту є важливим при проектуванні, моделюванні будь-якої КСЗІ, а також при встановленні стійкості СЗІ передбачуваному супротивникові. Для формування кожного обліку необхідно [8]:

–визначити математичний параметр, що характеризує об'єкт при його використовуваному математичному представленні, якісне застосування якого буде відмінним, залежно від характеру збурюючої дії;

–вибрати спосіб формального представлення атак на СЗІ так, щоб він, будучи простим в обчислювальному сенсі, дозволяв відобразити безпосередню спрямованість атаки;

–вибрати простий в обчислювальному сенсі спосіб представлення результата атаки.

Вирішення поставлених завдань дає можливість для створення моделі СЗІ, що дозволяє максимально швидко визначити наслідки організованої атаки, виділяючи «постраждалі» і «незаймані» засоби захисту.

Розробка математичної моделі об'єкту захисту неможлива без створення моделі передбачуваного супротивника [7,8].

Традиційним шляхом для представлення групи людей з відображенням взаємних стосунків між ними є використання теорії графів. Це обумовлено рядом чинників, серед яких наочність отримуваної моделі, можливість адекватного віддзеркалення за допомогою стандартних операцій на графах реальних дій над групами і подій у групах, існуванням розробленого математичного апарату для роботи з графами, включаючи велику кількість тих, що добре зарекомендували себе на практиці евристичних методів обробки.

Авторами пропонується загальна модель графів довільної групи супротивника із суворо обгрунтованим обліком ієрархії цієї групи за допомогою використання зваженого неорієнтованого графа, що, виходячи з [6,7,8] не використовувалося раніше.

Запропонована математична модель дає можливість для використання нових, не вживаних раніше, методів обробки графів для вирішення завдання про руйнування модельованого угрупування, а також чисельної оцінки збитку, що наноситься зловмисником.

Вирішення вказаних завдань і вимог дозволить створити прийнятний варіант системи захисту об'єкту, а вирішення відповідної сукупності завдань для всієї множини об'єктів створити варіант СЗІ для системи в цілому.

Вибір сукупності методів захисту об'єкту повинен проводиться з урахуванням певних каналів витоку для кожного конкретного об'єкту з метою їх перекриття. Потім для кожного окремого методу захисту повинна бути визначена вартість проектування та експлуатації при реалізації цього методу, вірогідність і вартість його злому, атаки або несанкціонованої дії. Наступні характеристики досить складні для визначення: оцінка вартості об'єкту, оцінки рівнів для кожного окремого методу захисту і рівня захисту самого об'єкту, а також оцінки величини втрат у разі несанкціонованого одержання інформації, нейтралізувавши кожен окремий метод захисту інформації. Тимчасові заборони, необхідні для подолання всіх методів, що застосовуються для захисту об'єкту, можуть бути отримані через вірогідність подолання кожного з методів і часу, необхідного для реалізації однієї спроби подолання кожного методу захисту.

Вказаними характеристиками є початкові дані, необхідні для створення і оцінки якості системи захисту кожного об'єкта і всієї системи і об'єкта в цілому.

Висновки

Виконання сформульованих вимог до системи захисту інформації дозволяє гарантувати, що будь-яке отримання і переміщення інформації на об'єкті захисту

ідентифікується, авторизується, виявляється, документується і при цьому забезпечується необхідний або заданий рівень її захищеності.

Список літератури

1. *Хорошко В.А.* – Методы и средства защиты информации/ Хорошко В.А., Чекатов А.А. – К.: Изд. Юниор, 2003. -504с.

2. *Ленков С.В.* – Методы и средства защиты информации. В 2-х томах/ Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

3. *Домарев В.В.* – Безопасность информационных технологий. Методология создания систем защиты/ Домарев В.В. – К.: ООО «ТИД» ДС», 2001. -688с.

4. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6. *Егоров Ф.И.* – Задачи защиты информации/ Егоров Ф.И., Тискина Е.О., Хорошко В.А.// Захист інформації, №1, 2009. –с.5-12.

7. *Невойт Я.В.* – Модель потенциально-опасной группы для предупреждения утечки информации/ Невойт Я.В., Мазуренко Л.Н, Хорошко В.А., Чередниченко В.С.// Системи обробки інформації, вип.7 (79), 2009. -с.82-86.

8. *Кобозева А.А.* – Анализ информационной безопасности/ Кобозева А.А., Хорошко В.А. – К.: Изд. ГУИКТ, 2009. -251с.

У роботі розроблені вимоги до систем захисту інформації, які розробляються для захисту об'єктів. Наведена сукупність вимог до систем захисту і запропонований порядок проведення робіт.
Ключові слова: система захисту інформації, несанкціонований доступ.

В работе разработаны требования к системам защиты информации, которые разрабатываются для защиты объектов. Приведена совокупность требований к системам защиты и предложен порядок проведения работ.

Ключевые слова: система защиты информации, несанкционированный доступ.

The requirements to information security systems for objects defence are developed in the article. A set of requirements to the systems of defence is resulted and the order of operations is offered.
Key words: information security, unauthorized access.

Надійшла 13.05.2010

УДК 004.4

к.т.н., доцент Козюра В.Д., (ГУИКТ)
Юрх Н.Г. (НА СБ Украины)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, БАЗИРУЮЩАЯСЯ НА ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Для описания технологии защиты информации конкретной информационной системы строится Политика информационной безопасности (ПИБ), которая представляет собой набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации. По сути – это совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. На основе ПИБ строится управление, защита и распределение критической информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение информационной системы в различных ситуациях.

Целью разработки ПИБ является определение правильного (с точки зрения организации) способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности.