– формування системи звіту щодо клієнтів і потенційних сегментів.

Питання для самоперевірки

1. Вимоги до програмних засобів маркетингу.
2. Назвіть, за якими класами поділяються програмні продукти для маркетингу.
3. Особливості корпоративних інформаційних систем.
4. Охарактеризуйте корпоративну інформаційну систему Baan».
5. Програма «Галактика».
6. Назвіть спеціалізовані програмні продукти, які дозволяють розв'язувати задачі з управління маркетингом.
7. Які саме програмні продукти використовуються під час проведення маркетингових досліджень? Охарактеризуйте їх.
8. Які саме програмні продукти використовуються під час моделювання стану ринку? Охарактеризуйте їх.
9. Назвіть програми, що мають маркетингову складову для розв'язання задач з управління маркетингом.

ТЕМА 9. Захист інформації

План

1. Значення інформації та її захисту.
2. Основні поняття захисту інформації й інформаційної безпеки.
3. Основи систем захисту інформації.
4. Основні аспекти інформаційної безпеки.
5. Класифікація методів захисту даних.
6. Файли й бази даних як інформаційні об'єкти захисту.
7. Управління захистом інформаційних об'єктів.

Інформаційні джерела

1. Купріянов А. І. Основи захисту інформації : навч. посіб. для студ. вищ. навч. закладів / А. І. Купріянов, А. В. Сахаров, В. А. Шевцов. – Москва : Видавничий центр «Академія», 2006. – 256 с.

2. Попов Л. І. Основні принципи підвищення ефективності реалізації заходів щодо комплексного захисту інформації / Л. І. Попов, А. В. Зубарєв. – «Альтпресс», 2009. – 512 с.

1. Значення інформації та її захисту

Сучасний світ характеризується такою цікавою тенденцією, як постійне підвищення ролі інформації. Як відомо, всі виробничі процеси мають в своєму складі матеріальну і нематеріальну складові. Перша – це необхідне для виробництва устаткування, матеріали і енергія в потрібній формі (тобто, чим і з чого виготовляється предмет). Друга складова – технологія виробництва (тобто, як він виготовляється). В останнє сторіччя з'явилися багато таких галузей виробництва, які майже на 100 % складаються з однієї інформації, наприклад, дизайн, створення програмного забезпечення, реклама та інші. Яскравим прикладом значна ролі інформації у виробничих процесах – це поява у XX ст. такого заняття, як промислове шпигунство. Не матеріальні цінності, а чиста інформація стає об'єктом викрадання.

У минулі століття людина використовувала знаряддя праці і машини для обробки матеріальних об'єктів, а інформацію про процес виробництва тримала в голові. У XX ст. з'явилися машини для обробки інформації – комп'ютери, роль яких підвищується з кожним роком.

Інтернет сьогодні – це технологія, що кардинально міняє весь устрій нашого життя: темпи науково-технічного прогресу, характер роботи, способи спілкування. Ефективне застосування інформаційних технологій є загальновизнаним стратегічним чинником зростання конкурентоспроможності компанії. Багато підприємств у світі переходять до використання широких можливостей Інтернету й електронного бізнесу, невід'ємний елемент якого – електронні транзакції (по Інтернету та іншим публічним мережам).

Електронна комерція, продаж інформації в режимі он-лайн і багато інших послуг стають основними видами діяльності для багатьох компаній, а їх корпоративні інформаційні системи (КІС) – головним інструментом управління бізнесом і, фактично, найважливішим засобом виробництва.

Важливим чинником, що впливає на розвиток КІС підприємства, є підтримка масових і різноманітних зв'язків підприємства через Інтернет з одночасним забезпеченням безпеки цих комунікацій. Тому вирішення проблем інформаційної безпеки, пов'язаних із широким розповсюдженням Internet, Intranet і Extranet, – одне з найактуальніших завдань, що стоять перед розробниками й постачальниками інформаційних технологій.

Завдання забезпечення інформаційної безпеки КІС традиційно вирішується побудовою системи інформаційної безпеки (СІБ), визначальною вимогою до якої є збереження вкладених у побудову КІС інвестицій. Створювана СІБ підприємства повинна враховувати появу нових технологій і сервісів, а також задовольняти загальним вимогам, що пред'являються сьогодні до будь-яких елементів КІС, таким як:

- застосування відкритих стандартів;
- використання інтегрованих рішень;
- забезпечення масштабування в широких межах.

Перехід на відкриті стандарти складає одну з головних тенденцій розвитку засобів інформаційної безпеки. Такі стандарти як IPSec і PKI забезпечують захищеність зовнішніх комунікацій підприємств і сумісність з відповідними продуктами підприємств-партнерів або видалених клієнтів. Цифрові сертифікати X.509 також є на сьогодні стандартною основою для аутентифікації користувачів і пристроїв. Перспективні засоби захисту, безумовно, повинні підтримувати ці сьогоднішні стандарти.

Під інтегрованими рішеннями розуміється як інтеграція засобів захисту з рештою елементів мережі (ОС, маршрутизаторами, службами каталогів і т. ін.), так і інтеграція різних технологій безпеки між собою для забезпечення комплексного захисту інформаційних ресурсів підприємства, наприклад інтеграція міжмережевого екрану з VPN-шлюзом і транслятором IP-адрес.

У міру зростання і розвитку КІС система інформаційної безпеки повинна мати можливість легко масштабуватися без втрати цілісності і керованості. Для того, щоб забезпечити надійний захист ресурсів КІС, у СІБ повинні бути реалізовані най-

прогресивніші й перспективніші технології інформаційного захисту. До них належать:

– криптографічний захист даних для забезпечення конфіденційності, цілісності й достовірності інформації;

– технології аутентифікації для перевірки достовірності користувачів і об'єктів мережі;

– технології міжмережевих екранів для захисту корпоративної мережі від зовнішніх погроз під час підключення до загальнодоступних мереж зв'язку;

– технології віртуальних захищених каналів і мереж VPN для захисту інформації, передаваної по відкритих каналах зв'язку;

– гарантована ідентифікація користувачів шляхом застосування токенов (смарт-карт, touchmemory, ключів для USB-портів) та інших засобів аутентифікації;

– управління доступом на рівні користувачів і захист від несанкціонованого доступу до інформації;

– підтримка інфраструктури управління відкритими ключами PKI;

– технології виявлення вторгнень (Intrusion Detection) для активного дослідження захищеності інформаційних ресурсів;

– технології захисту від вірусів із використанням спеціалізованих комплексів антивірусної профілактики й захисту;

– централізоване управління СІБ на базі єдиної політики безпеки підприємства;

– комплексний підхід до забезпечення інформаційної безпеки, що забезпечує раціональне поєднання технологій і засобів інформаційного захисту.

2. Основні поняття захисту інформації й інформаційної безпеки

Сучасні методи обробки, передачі та накопичення інформації сприяли появі погроз, пов'язаних із можливістю втрати, спотворення і розкриття даних, що адресовані або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним із провідних напрямів розвитку IT.

Розглянемо основні поняття захисту інформації та інформаційної безпеки комп'ютерних систем і мереж.

Захист інформації – це діяльність по запобіганню просочуванню інформації, що захищається, несанкціонованих і ненавмисних дій з інформацію, що захищається.

Об'єкт захисту – інформація, носій інформації або інформаційний процес, відносно яких необхідно забезпечувати захист відповідно до поставленої мети захисту інформації. Мета захисту інформації – це бажаний результат захисту інформації. Метою захисту інформації може бути запобігання збитку власникові, користувачеві інформації в результаті можливого просочування інформації і/або несанкціонованої і ненавмисної дії на інформацію.

Ефективність захисту інформації – ступінь відповідності результатів захисту інформації поставленій мети.

Захист інформації від витоку – діяльність із запобігання неконтрольованому розповсюдженню інформації, що захищається, від її розголошування, несанкціонованого доступу (НСД) до інформації, що захищається, і отримання інформації, що захищається, зловмисниками.

Захист інформації від розголошування – діяльність із запобігання несанкціонованому доведенню інформації, що захищається, до неконтрольованої кількості одержувачів інформації.

Захист інформації від НСД – діяльність по запобіганню, отриманню інформації, що захищається, зацікавленим суб'єктом із порушенням установлених правових документів або правил доступу до інформації, що захищається. Зацікавленим суб'єктом, що здійснює НСД до інформації, що захищається, може виступати держава, юридична особа, група фізичних осіб, у тому числі громадська організація, окрема фізична особа.

Система захисту інформації – сукупність органів і/або виконавців, використовувана ними техніка захисту інформації, а також об'єкти захисту, організовані й такі, що функціонують за правилами, установленими відповідними правовими, організаційно-розпорядчими й нормативними документами із захисту інформації.

Під інформаційною безпекою розуміють захищеність інформації від незаконного ознайомлення, перетворення і знищення, а також захищеність інформаційних ресурсів від дій, направлених на порушення їх працездатності. Природа цих дій може бути найрізноманітнішою. Це і спроби проникнення зловмисників, і помилки персоналу, і вихід із ладу апаратних і програмних засобів, і стихійні лиха (землетрус, ураган, пожежа) тощо.

Сучасна автоматизована система (АС) обробки інформації є складною системою, що складається з великого числа компонентів різного ступеня автономності, які пов'язані між собою й обмінюються даними. Практично кожен компонент може піддатися зовнішній дії або вийти з ладу.

Компоненти АС можна розбити на такі групи:

– апаратні засоби – комп'ютери та їх складові частини (процесори, монітори, термінали, периферійні пристрої – дисководи, принтери, контролери, кабелі, лінії зв'язку);

– програмне забезпечення – придбані програми, початкові, об'єктні, завантажувальні модулі ОС і системні програми (компілятори, компоновщики й ін.), утиліти, діагностичні програми;

– дані – що зберігаються тимчасово й постійно, на магнітних носіях, друкарські, архіви, системні журнали;

– персонал – обслуговувальний персонал і користувачі.

Однією з особливостей забезпечення інформаційної безпеки в АС є те, що таким абстрактним поняттям, як інформація, об'єкти й суб'єкти системи, відповідають фізичні уявлення в комп'ютерному середовищі:

– для представлення інформації – машинні носії інформації у вигляді зовнішніх пристроїв комп'ютерних систем (терміналів, друкуючих пристроїв, різних накопичувачів, ліній і каналів зв'язку), оперативної пам'яті, файлів, записів;

– об'єктам системи – пасивні компоненти системи, що зберігають, приймають або передають інформацію. Доступ до об'єкта означає доступ до інформації, що міститься в ньому;

– суб'єктам системи – активні компоненти системи, які можуть стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи. Як суб'єкти можуть виступати користувачі, активні програми і процеси.

Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності й достовірності оброблюваних даних, а також доступності й цілісності інформаційних компонентів і ресурсів системи. Вищеперераховані базові властивості інформації потребують повнішого тлумачення.

Конфіденційність даних – це статус, наданий даним, що визначає необхідний ступінь їх захисту.

До конфіденційних даних можна зарахувати, наприклад, такі: особисту інформацію користувачів;

облікові записи (імена й паролі); дані про кредитні карти; дані про розробки й різні внутрішні документи; бухгалтерські відомості. Конфіденційна інформація повинна бути відома тільки допущеним суб'єктам системи, що пройшли перевірку (авторизованим) (користувачам, процесам, програмам). Для решти суб'єктів системи ця інформація повинна бути невідомою.

Установлення градацій важливості захисту інформації (об'єкту захисту), що захищається, називають категоруванням інформації, що захищається.

Під цілісністю інформації розуміється властивість інформації зберігати свою структуру і/або зміст у процесі передачі та зберігання. Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в семантичному відношенні від даних у початкових документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування. Забезпечення цілісності даних є одним із складних завдань захисту інформації.

Достовірність інформації – властивість інформації, що виражається в строгій приналежності суб'єктові, який є її джерелом, або тому суб'єктові, від якого ця інформація прийнята.

Юридична значущість інформації означає, що документ, що є носієм інформації, має юридичну силу.

Доступність даних. Робота користувача з даними можлива тільки в тому випадку, якщо він має до них доступ.

Доступ до інформації – отримання суб'єктом можливості ознайомлення з інформацією, зокрема за допомогою технічних засобів.

Суб'єкт доступу до інформації – учасник правовідносин в інформаційних процесах.

Оперативність доступу до інформації – це здатність інформації або деякого інформаційного ресурсу бути доступними для кінцевого користувача відповідно до його оперативних потреб.

Власник інформації – суб'єкт, що в повному об'ємі реалізовує повноваження володіння, користування, розпорядження інформацією відповідно до законодавчих актів.

Користувач (споживач) інформації – суб'єкт, що користується інформацією, отриманою від її власника або посередника відповідно до встановлених прав і правил доступу до інформації або з їх порушенням.

Право доступу до інформації – сукупність правил доступу до інформації, установлених правовими документами або власником інформації.

Правило доступу до інформації – сукупність правил, що регламентують порядок та умови доступу суб'єкта до інформації і її носіїв.

Розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації – це доступ до інформації, що не порушує встановлені правила розмежування доступу. Правила розмежування доступу слугують для регламентації права доступу до компонентів системи.

Несанкціонований доступ до інформації – порушення встановлених правил розмежування доступу. Особа або процес, що здійснюють НСД до інформації, є порушниками правил розмежування доступу. НСД є найбільш поширеним видом комп'ютерних порушень.

Відповідальним за захист комп'ютерної системи від НСД до інформації є адміністратор захисту.

Доступність інформації має на увазі також доступність компонента або ресурсу комп'ютерної системи, тобто властивість компоненту або ресурсу бути доступним для законних суб'єктів системи.

Примірний перелік ресурсів, які можуть бути доступні,

включає: принтери, сервери, робочі станції, дані користувачів, будь-які критичні дані, необхідні для роботи.

Цілісність ресурсу або компонента системи – це властивість ресурсу або компонента бути незмінним у семантичному сенсі під час функціонування системи в умовах випадкових або навмисних спотворень або руйнуючих дій.

З допуском до інформації і ресурсів системи пов'язана група таких важливих понять, як ідентифікація, аутентифікація, авторизація. З кожним суб'єктом системи (мережі) пов'язують деяку інформацію (число, рядок символів), що ідентифікує суб'єкт. Ця інформація є ідентифікатором суб'єкта системи (мережі). Суб'єкт, що має зареєстрований ідентифікатор, є законним (легальним) суб'єктом.

Ідентифікація суб'єкта – це процедура розпізнавання суб'єкта за його ідентифікатором. Ідентифікація виконується за спроби суб'єкта увійти до системи (мережі). Наступним кроком взаємодії системи із суб'єктом є аутентифікація суб'єкта. Аутентифікація суб'єкта – це перевірка достовірності суб'єкта з даним ідентифікатором.

Процедура аутентифікації встановлює, чи є суб'єкт саме тим, ким він себе оголосив. Після ідентифікації й аутентифікації суб'єкта виконують процедуру авторизації.

Авторизація суб'єкта – це процедура надання законному суб'єктові, що успішно пройшов ідентифікацію й аутентифікацію, відповідних повноважень і доступних ресурсів системи (мережі).

Під загрозою безпеки АС розуміються можливі дії, здатні прямо або побічно завдати збитку її безпеці. Збиток безпеки має на увазі порушення стану захищеності інформації, що міститься й обробляється в системі (мережі). З поняттям загрози безпеки тісно пов'язано поняття уразливості комп'ютерної системи (мережі). Уразливість комп'ютерної системи – це властива системі невдала властивість, яка може призвести до реалізації загрози. Атака на комп'ютерну систему – це пошук і/або використання зловмисником тієї або тієї вразливості системи. Іншими словами, атака – це реалізація загрози безпеці.

Протидія загрозам безпеці є метою засобів захисту комп'ютерних систем і мереж.

Захищена система – це система із засобами захисту, які успішно й ефективно протистоять погрозам безпеці.

Спосіб захисту інформації – порядок і правила застосування певних принципів і засобів захисту інформації.

Засіб захисту інформації – технічний, програмний засіб, речовина і/або матеріал, призначені або використовувані для захисту інформації.

Комплекс засобів захисту (КЗЗ) – сукупність програмних і технічних засобів, що створюються і підтримуються для забезпечення інформаційної безпеки системи (мережі). КЗЗ створюється і підтримується відповідно до прийнятої в даній організації політики безпеки.

Техніка захисту інформації – засоби захисту інформації, засоби контролю ефективності захисту інформації, засоби і системи управління, призначені для забезпечення захисту інформації.

Корпоративні мережі належать до розподілених автоматизованих систем (АС), що здійснюють обробку інформації. Забезпечення безпеки АС припускає організацію протидії будь-якому несанкціонованому вторгненню у процес функціонування АС, а також спробам модифікації, розкрадання, виведення з ладу або руйнування її компонентів, тобто захист усіх компонентів АС – апаратних засобів, програмного забезпечення (ПО), даних і персоналу. Конкретний підхід до проблеми забезпечення безпеки заснований на розробленій для АС політиці безпеки.

Політика безпеки – це сукупність норм, правил і практичних рекомендацій, що регламентують роботу засобів захисту комп'ютерної системи від заданої безлічі погроз.

3. Основи систем захисту інформації

Захист інформації в ІС – це регулярне використання засобів і методів, здійснення заходів із метою системного забезпечення необхідної надійності інформації, яку зберігають та обробляють із використанням ІС.

Конфіденційність – характеристика інформації, що вказує на необхідність уведення обмежень на коло суб'єктів, які мають доступ до даної інформації. Ця властивість забезпечується спроможністю системи зберігати зазначену інформацію в таємниці від суб'єктів, що не мають повноважень на доступ до неї.

Власне кажучи, погрозами порушення конфіденційності є такі погрози, що можуть призвести або призводять до несанкціонованого ознайомлення з інформацією, що захищається.

Безпека – захищеність інформації від небажаного розголошення (порушення конфіденційності), перекручування (порушення цілісності), втрати або зниження ступеня доступності, незаконного тиражування.

Цілісність представляє властивість, що забезпечує умови введення таких інформаційних відносин між суб'єктами й об'єктами, за яких інформація зберігається для використання і виконує свої основні функції. Погрози, що належать до несанкціонованої модифікації інформації, є погрозами порушення цілісності. У результаті успішної реалізації погрози порушення цілісності об'єктам і суб'єктам наноситься або може бути нанесений неприпустимий збиток.

Доступність є властивістю, що забезпечує своєчасний і якісний доступ санкціонованих об'єктів і суб'єктів до інформації і ресурсів інформаційної системи. Як одна з послуг забезпечення безпеки вона потенційно піддана атакам, спрямованим на те, щоб зробити ресурси або інформацію, а також послуги інформаційної системи незадовільними або зі зниженою якістю. Такі атаки наносять або можуть завдавати неприпустимої шкоди.

Спостережність (керування доступом) полягає в забезпеченні можливості доступу до інформації і/або до ресурсів системи тільки об'єктам і суб'єктам, що володіють відповідними повноваженнями, та відстеженні їхніх дій усередині системи. До погроз порушення спостережності зараховують погрози, що призводять до погіршення керування і контролю доступом, маніпулювання системою, ресурсами або інформацією. Для керування доступом використовується термін тег, що позначає деяку інформацію, яка використовується для керування доступом і пов'язана з користувачами, процесами або об'єктами.

Надійність інформації в ІС – це інтегральний показник, що характеризує якість інформації з погляду:

1) фізичної цілісності, тобто наявності (відсутності) перекручувань або знищення елементів цієї інформації;

2) довіри до інформації (автентичності), тобто відсутності в ній підміни (несанкціонованої модифікації) її елементів за умови збереження цілісності;

3) безпеки інформації (конфіденційності), тобто відсутності несанкціонованого одержання її особами або процесами, що не мають на це повноважень;

4) недопущення несанкціонованого розмноження інформації.

Ефективність захисту інформації в ІС досягається лише в тому випадку, якщо забезпечується її надійність на всіх об'єктах і елементах системи, що можуть бути піддані погрозам із боку зовнішнього середовища.

Об'єкт захисту – такий структурний компонент системи, у якому знаходиться або може знаходитися інформація, яка підлягає захисту.

Система захисту інформації (СЗІ) – комплекс організаційних заходів і програмно-технічних (у тому числі криптографічних) засобів забезпечення безпеки інформації в автоматизованих системах.

Політика безпеки – набір законів, правил і практичного досвіду, на основі яких будується управління, захист і розподіл критичної інформації.

У сучасних умовах спостерігається цілеспрямований усебічний вплив на інформаційні ресурси, тому у складі ІС необхідно передбачити комплексну систему захисту інформації, до якої повинні бути включені:

структурні органи (із визначеною ієрархією), що здійснюють розробку контроль виконання нормативних і керівних документів щодо забезпечення захисту інформації;

сукупність різних методів (фізичних, організаційних, криптографічних) і засобів (програмних, апаратних, апаратно-програмних), що забезпечують повний захист апаратного й програмного забезпечення інформаційних систем, а також безпеку та контроль самих систем захисту.

Питання організації захисту інформації повинні вирішуватися вже на проектній стадії розробки ІС. Похибки захисту можуть бути значною мірою усунуті, якщо під час проектування враховувати такі основні принципи побудови системи захисту:

1. Простота механізму захисту. Механізми захисту повинні бути інтуїтивно зрозумілі та прості у використанні.

2. Постійність захисту. Надійний механізм, який реалізує цю вимогу, повинен бути постійно захищений від несанкціонованих змін.

3. Контроль повинен бути повним. Цей принцип припускає необхідність перевірки повноваження будь-якого звертання до будь-якого об'єкта.

4. Несекретність проектування – механізм захисту повинен працювати досить ефективно, навіть якщо його структура та зміст відомі зловмиснику. Ефективність захисту не повинна залежати від того, наскільки досвідчені потенційні порушники.

5. Ідентифікація. Кожний об'єкт ІС повинен однозначно ідентифікуватися. Під час спроби одержання доступу до інформації рішення про його санкціонування необхідно приймати на підставі даних претендента й найвищого ступеня таємності інформації, із яким він може працювати.

6. Поділ повноважень застосування декількох ключів захисту, що зручно, якщо право на доступ визначається виконанням ряду умов.

7. Мінімальні повноваження. Для будь-якої програми й будь-якого користувача повинне бути визначене мінімальне коло необхідних повноважень.

8. Надійність. Система захисту інформації повинна мати механізм оцінювання надійності функціонування СЗІ.

9. Максимальна відособленість механізму захисту означає, що захист повинний бути відділений від функцій управління даними.

10. Захист пам'яті. Пакет програм, що реалізують захист, повинен розміщатися в захищеному полі пам'яті комп'ютера, щоб забезпечити системну локалізацію спроб проникнення ззовні.

11. Зручність для користувачів. Механізм захисту не повинен створювати для користувачів додаткових труднощів.

12. Авторизація користувача на основі фізичного ключа й особистого PIN-коду дозволяє виключити ненавмисну дискредитацію його прав доступу.

13. Звітність. Необхідно захищати контрольні дані від модифікації і несанкціонованого знищення, щоб забезпечити виявлення і розслідування виявлених фактів порушення безпеки.

14. Доступність до виконання тільки тих команд операційної системи, що не можуть ушкодити операційне середовище.

15. Системний підхід до захисту інформації припускає необхідність обліку всіх взаємозалежних, взаємодіючих її елементів, що змінюються в часі, умов і чинників, які мають істотну значимість для забезпечення безпеки ІС.

16. Можливість нарощування. Під час побудови системи захисту повинні враховуватися можливості появи принципово нових шляхів реалізації погроз безпеки.

17. Комплексний підхід припускає погоджене застосування різнорідних засобів захисту інформації.

18. Адекватність забезпечення необхідного рівня захисту (визначається ступенем таємності інформації, що підлягає опрацюванню) за мінімальних витрат на створення механізму захисту й забезпечення його роботи.

19. Карність порушень. Найбільш поширена міра покарання – відмова в доступі до системи.

20. Економічність механізму – забезпечення мінімальності витрат на створення та експлуатацію механізму.

21. Спеціалізованість надійний механізм захисту може бути спроектований та організований лише професійними фахівцями із захисту інформації.

22. Гнучкість системи захисту забезпечує можливість варіювання рівнем захищеності ІС.

23. Принцип неперервності захисту припускає, що захист інформації – це неперервний цілеспрямований процес, що припускає прийняття відповідних заходів на всіх етапах життєвого циклу ІС.

4. Основні аспекти інформаційної безпеки

Відзначимо аспекти проблеми безпеки (рис. 28):

Рисунок 28 – Основні аспекти інформаційного забезпечення

Правові, суспільні та етичні аспекти (чи має право деяка особа одержати запитувану інформацію, наприклад, про кредит клієнта).

Фізичні умови (закриті або захищені іншим чином даний комп'ютер і термінальна кімната).

Організаційні питання (як у межах підприємства, що володіє деякою системою, організовано доступ до даних).

Питання реалізації управління (наприклад, як часто змінюються паролі).

Апаратне забезпечення (чи забезпечується проведення заходів безпеки на апаратному рівні, наприклад, за допомогою захисних ключів або привілейованого режиму управління).

Безпека операційної системи (наприклад, чи затирає базова операційна система зміст структури збереження і файлів із даними в разі припинення роботи з ними).

5. Класифікація методів захисту даних

Важливо розрізняти три види ЗІ – захист інформації, безвідносно до того, де вона знаходиться, захист носіїв і захист безпосередньо комп'ютера.

Методи захисту інформації можна розділити на дві групи: апріорні й апостеріорні. До апріорних методів захисту інформації належать методи забезпечення повноти і достовірності даних на етапі підготовки і введення інформації в комп'ютер. До апостеріорних методів захисту інформації відноситься використання вбудованих засобів захисту даних в операційних системах і різних додатках, парольний захист інформації, архівація, захист інформації від вірусів і використання криптографії, тобто, шифровка даних. Другий тип включає декілька методів захисту носіїв інформації, їх можна підрозділити на програмні, апаратні й комбіновані.

Програмний метод перешкоджає доступу до конкретного носія або до комп'ютера цілком.

Наприклад, пароль на CMOS.

Програмно-апаратний метод із використанням електронних ключів, які найчастіше вставляються в COM-порт ПК. Не отримуючи потрібну відповідь від ключа, програма, для якої він призначений, не працюватиме або не надаватиме користувачеві доступ до своїх даних. Методи захисту ПК включають спеціальні засоби для усунення просочування інформації і засобу захисту від апаратних збоїв.

Методи захисту даних на етапі введення в інформаційні системи (апріорний захист інформації).

До цих методів належать методи контролю і попередження помилок операторів під час уведення даних в інформаційні системи.

Метод контрольних сум

Цей метод використовується для виявлення помилок під час уведення числової інформації. Суть методу полягає в наступ-

ному. Перед уведенням уся числова інформація підсумовується по рядках і стовпцях. Отримані результати вносяться до бланка введення даних у вигляді додаткового стовпця і рядка. У разі введення даних програмним шляхом виконується контрольне підсумовування даних, що вводяться, за рядками та стовпцями. Отримані результати порівнюються з введеними значеннями контрольних сум за рядками та стовпцями. У разі виявлення неспівпадіння введеного значення контрольної суми й розрахованого значення контрольної суми видається повідомлення про помилку. За наявності однієї помилки в терміні та стовпці помилкове число знаходиться на перетині рядка та стовпця, у яких видано повідомлення про помилку.

Метод подвійного введення даних

Цей метод може бути використаний для виявлення помилок під час уведення будь-яких даних. У ході використання даного методу одна й та ж інформація вводиться в комп'ютер двома різними операторами. Потім ця інформація порівнюється в комп'ютері програмним шляхом. У разі виявлення неспівпадіння даних видається інформація про помилку.

Накладення обмежень та умов на дані, що вводяться

Під час уведення даних в інформаційних системах широко використовуються обмеження на введення даних. Наприклад, можна обмежити дані, уведення яких допускається в полі, визначивши для цього поля умову на значення. Якщо дані, що вводяться в поле, не відповідають заданій умові, то на екран буде виведено повідомлення, яке сповіщає про те, які дані дозволено вводити в указане поле. Ще одним способом управління введенням даних є створення маски введення, яка обмежує вид значень, що вводяться в певні позиції в полі. Ці прості способи перевірки умов на значення й обмеження можна реалізувати, установивши властивості для полів у таблицях або для елементів управління у формах.

6. Файли й бази даних як інформаційні об'єкти захисту

Інформаційні об'єкти ІС – це будь-яка інформація (повідомлення, відомості, файли бази даних) в будь-яких формах її подання (аналогова, цифрова, віртуальна, уявна).

Коли розглядаються процедури захисту мережних баз даних, то дані та їх логічні структури представляються двома способами. Окремі об'єкти даних самі можуть бути об'єктами захисту або можуть бути організовані у структури БД (сегменти, відношення, каталоги).

Колективне використання файлів визначає необхідність в організації їх захисту від несанкціонованого використання, а також від фізичної руйнації. Проблема ускладнюється у зв'язку з тим, що користувачі можуть давати свої файли іншим користувачам. Отже, усі файли, що захищаються, можна умовно класифікувати так: загальні, групові, особисті.

Для забезпечення цілісності файлів можуть бути використані апаратні та програмні засоби захисту, а також сукупність заходів організаційного плану, що дозволяють проводити облік, збереження і використання файлів.

Організація збереження і використання інформації в базах даних (БД) має специфічні особливості. Якщо до інформації, що міститься в БД, звертається багато користувачів, то особливо важливо, щоб елементи даних і зв'язки між ними не руйнувалися. Необхідно також враховувати можливість виникнення помилок і різного роду випадкових збоїв. Збереження, відновлення і процедури включення даних повинні бути такими, щоб система у випадку виникнення збоїв могла відновлювати дані без утрат.

Захист БД означає захист власне даних і їх контрольоване використання на робочих місцях мережі, а також захист будь-якої супутньої інформації, що генерується з цих даних. Управління даними під час організації захисту інформаційних баз, що застосовують різні механізми захисту та криптографічні ключі в якості даних, увійшли у процедури захисту об'єктів ІС. Захист даних у процесі передачі між вузлами мережі здійснюється за допомогою процедур захисту ліній зв'язку.

Функції, процедури й засоби захисту, що забезпечують захист даних на робочих станціях мережі, можна описати в такий спосіб:

1. Захист змісту даних об'єднує функції, процедури й засоби захисту, що попереджують несанкціоноване розкриття конфіденційної інформації з БД.

2. Засоби контролю доступу дозволяють доступ до даних тільки повноважним суб'єктам відповідно до строго визначених правил та умов.

3. Управління потоком захищених даних під час передачі з одного сегмента БД в інший забезпечує переміщення даних разом із механізмами захисту, властивими вихідним даним.

4. Контроль узгодженості під час використання БД припускає процедури захисту, що забезпечують захист і цілісність окремих елементів даних.

5. Контекстний захист даних, характерний для схем захисту динамічних БД, також повинен бути включений до складу процедур захисту БД.

6. Запобігання створення несанкціонованої інформації припускає наявність засобів, які попереджають, що об'єкт одержує (генерує) інформацію, котра перевищує рівень прав доступу, і здійснює це, використовуючи логічний зв'язок між даними в БД.

Терміни *безпека й цілісність* у контексті обговорення баз даних часто використовуються сумісно, хоча насправді, це різні поняття. Термін безпека стосується захисту даних від несанкціонованого доступу, зміни або руйнації даних, а цілісність – точності або істинності даних.

Тобто під безпекою мається на увазі, що користувачам дозволяється виконувати деякі дії; під цілісністю мається на увазі, що ці дії виконуються коректно.

Між цими термінами є, звичайно, деяка подібність, оскільки як під час забезпечення безпеки, так і під час забезпечення цілісності система змушена перевірити, чи не порушують дії користувача деякі правила. Ці правила повинні бути задані адміністратором бази даних (АБД) певним чином і збережені в системному каталозі. Причому в обох випадках система управління базою даних (СКБД) повинна якимось способом відслідковувати всі дії користувача й перевіряти їх на відповідність заданим правилам.

7. Управління захистом інформаційних об'єктів

Управління захистом – це контроль за розподілом інформації в інформаційних системах. Він здійснюється для забезпечення

функціонування засобів і механізмів захисту; фіксації виконуваних функцій і станів механізмів захисту і фіксації подій, пов'язаних із порушенням захисту.

Аналіз цілісності системи захисту інформації (СЗІ) ґрунтується на постійному вивченні протоколів (як машинних, так і ручних), перевірці аварійних сигналізаторів та інших пристроїв. За проведення аналізу відповідальність несе співробітник, що займається питаннями забезпечення цілісності.

Прилади аварійної сигналізації доцільно перевіряти досить часто, але не в точно встановлений час. До числа цих приладів належать детектори вогню і диму, датчики вологості й температури, апаратура сигналізації під час спроб проникнення в помешкання, пристрої фізичного контролю доступу, дверна сигналізація й інші аналогічні прилади.

Побічним продуктом аналізу цілості може виявитися статистична оцінка ефективності використання ПК та оцінка ефективності роботи користувачів. На основі результатів перевірки проводяться щотижневі наради, на яких заслуховується повідомлення співробітника, відповідального за забезпечення цілісності.

Крім звичайних регулярних перевірок, співробітник, відповідальний за забезпечення цілісності, зобов'язаний виконувати тестовий контроль перевірки апаратури та програмного забезпечення і фіксувати результати тестування.

Після вибору надійних засобів захисту необхідно налаштувати їх так, щоб усі вимоги політики безпеки виконувалися так, як зафіксовано у плані захисту.

Якщо кожний користувач працює автономно, вирішує тільки індивідуальні задачі та обробляє лише власні дані, то ізоляція користувачів та індивідуальний захист є досить надійними. Наявність будь-яких ресурсів, які сумісно використовуються і є доступними для модифікації, створює передумови порушення політики безпеки. Ця обставина, у свою чергу, породжує проблему взаємної недовіри: якщо декілька користувачів мають однакові права на якийсь набір даних, то хто відповідатиме, якщо з ним щось трапиться?