6.3. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В УПРАВЛІНСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

До основних методів захисту інформації в ІС відносяться: перешкода, управління доступом, маскування, регламентація, примушення, спонукання.

Перешкода - метод фізичного перешкодження шляху зловмисникові до інформації, що потребує захисту.

Управління доступом - метод захисту інформації шляхом регулювання використання всіх ресурсів інформаційної системи (елементів баз даних, програмних і технічних засобів). Управління доступом включає наступні функції захисту:

- ідентифікацію користувачів, персоналу і ресурсів системи;
- пізнання об'єкта або суб'єкта по пред'явленому ним ідентифікатору;
- перевірку повноважень;
- дозвіл і створення умов роботи в межах встановленого регламенту;
- реєстрацію звернень до ресурсів, що захищаються;
- реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Маскування - метод захисту інформації шляхом її криптографічного закриття.

Регламентація - метод захисту інформації, що створює такі умови автоматизованої обробки, зберігання і передачі інформації, що потребує захисту, при яких можливості несанкціонованого доступу до неї зводилися б до мінімуму.

Примушення - такий метод захисту, при якому користувачі і персонал системи вимушені дотримувати правила обробки, передачі і використання інформації, що потребує захисту, під загрозою матеріальної, адміністративної або кримінальної відповідальності.

Спонукання - такий метод захисту, який спонукає користувача і персонал системи не порушувати встановлені порядки за рахунок дотримання моральних і етичних норм, що склалися.

До основних засобів захисту відносяться:

- технічні засоби, що реалізовуються у вигляді електричних, електромеханічних і електронних пристроїв. Всю сукупність технічних засобів прийнято ділити на апаратні і фізичні. Під апаратними засобами розуміють пристрої, що вбудовуються безпосередньо в обчислювальну техніку або пристрої, які сполучаються з подібною апаратурою через стандартний інтерфейс. До фізичних засобів відносяться автономні пристрої і системи (замки на дверях, де розміщена апаратура, грати на вікнах, електронно-механічне устаткування охоронної сигналізації);
- програмні засоби, спеціально призначені для виконання функцій захисту інформації;
- організаційні засоби захисту (організаційно-технічні і організаційно-правові заходи, що здійснюються в процесі створення і експлуатації обчислювальної техніки, апаратура телекомунікацій для забезпечення захисту інформації);
- морально-етичні засоби захисту реалізуються у вигляді всіляких норм, які склалися традиційно або складаються у міру розповсюдження обчислювальної техніки і засобів зв'язку в суспільстві (прикладом таких норм є Кодекс професійної поведінки членів Асоціацій користувачів ЕОМ США);
- законодавчі засоби захисту, котрі визначені законодавчими актами країни, якими регламентуються правила користування, обробки і передачі інформації обмеженого доступу і встановлюються заходи відповідальності за порушення цих правил.

Для реалізації заходів безпеки використовуються різні механізми криптографії, тобто науки користувач одержує це повідомлення, він дешифрує або розкриває його за допомогою зворотного перетворення криптограми.

Криптографічна система ґрунтується на використанні спеціального алгоритму, який запускається унікальним числом, так званим, шифруючим про забезпечення секретності і достовірності переданих повідомлень.

Суть криптографічних методів полягає в тому, що для запобігання несанкціонованому доступу до будь-якого повідомлення, воно зашифровується. В разі, якщо санкціонований ключем. Для обміну зашифрованими повідомленнями як відправникові, так і одержувачу необхідно знати правильну ключову установку і зберігати її в таємниці.

Шифрування може бути симетричним і асиметричним: перше ґрунтується на використанні одного і того ж секретного ключа для шифрування і дешифровки, друге характеризується тим, що для шифрування використовується один ключ, що є загальнодоступним, а для дешифровки - інший, що є секретним.

Разом з шифруванням використовуються й інші механізми безпеки:

- цифровий (електронний) підпис;
- контроль доступу;
- забезпечення цілісності даних;
- забезпечення аутентифікації;
- управління маршрутизацією;
- арбітраж або огляд.

Механізми цифрового підпису ґрунтуються на алгоритмах асиметрічного шифрування і включають дві процедури: формування підпису відправником та її пізнання (верифікацію) одержувачем.

Механізми контролю доступу здійснюють перевірку повноважень об'єктів ІС на доступ до ресурсів мережі.

Механізми забезпечення цілісності даних реалізуються виконанням взаємозв'язаних процедур шифрування і дешифровки відправником і одержувачем. Відправник доповнює блок, що передається криптографічною сумою, а одержувач порівнює її з криптографічним значенням, відповідним прийнятому блоку. Неспівпадання свідчить про спотворення інформації в блоці.

Механізми управління маршрутизацією забезпечують вибір маршрутів руху інформації по комунікаційній мережі так, щоб виключити передачу секретних відомостей по фізично ненадійних каналах.

Механізми арбітражу забезпечують підтвердження характеристик даних, що передаються між об'єктами ІС, третьою стороною (арбітром).

Види захисту в економічних інформаційних системах класифікуються за напрямами захисту. До основних з них відносяться:

- захист інформації від несанкціонованого доступу;
- захист інформації в системах зв'язку;
- захист юридичної значущості електронних документів;
- захист конфіденційної інформації від витоку по каналах побічних електромагнітних випромінювань і наведень;
- захист інформації від комп'ютерних вірусів та інших небезпечних дій по каналах розповсюдження програм;
- захист від несанкціонованого копіювання і розповсюдження програм і цінної комп'ютерної інформації.

З погляду захисту інформації несанкціонований доступ може мати наступні наслідки: витік конфіденційної інформації, що опрацьовується, а також її руйнування в результаті умисного порушення працездатності ІС.

Одним з основних видів захисту інформації від несанкціонованого доступу є розмежування повноважень і доступу до інформації.

Іншим з усіх ефективних методів забезпечення безпеки ІС є реєстрація. З цією метою ведеться реєстраційний журнал, в який фіксуються всі здійснені або нездійснені спроби доступу до даних або програм.

Система реєстрації і обліку здійснює:

- реєстрацію входу (виходу) суб'єктів доступу в систему (з системи) або реєстрацію завантаження та ініціалізації операційної системи, а також її програмних установок;
- реєстрацію і облік видачі друкарських (графічних) документів;
- реєстрацію запуску (завершення) програм і процесів (завдань), призначених для обробки захищених файлів;
- реєстрацію спроб доступу програмних засобів захищених файлів;
- облік всіх носіїв захисту інформації.

До видів захисту інформації в системах зв'язку відносяться застосування криптографії та спеціальних зв'язкових протоколів.

До видів захисту юридичної значущості електронних документів відноситься застосування «цифрового підпису», який є одним з криптографічних методів перевірки достовірності інформаційних об'єктів.

Для захисту від побічних електромагнітних випромінювань і наведень застосовується екранування приміщень, призначених для розміщення засобів обчислювальної техніки, а також технічні заходи, що дозволяють понизити інтенсивність інформативних випромінювань ЕОМ і засобів зв'язку.

Видами захисту інформації від комп'ютерних вірусів та інших небезпечних дій по каналах розповсюдження програм є:

- «імуностійкі» програмні засоби, захищені від можливості несанкціонованої модифікації (розмежування доступу, методи самоконтролю і самовідновлення);

- спеціальні програми-аналізатори, що здійснюють постійний контроль виникнення відхилень в роботі прикладних програм, періодичну перевірку наявності інших можливих слідів вірусної активності, а також вхідний контроль нових програм перед їх використанням.

Захист від несанкціонованого копіювання і розповсюдження програм і цінної комп'ютерної інформації здійснюється за допомогою спеціальних програмних засобів, що піддають програми захисту, і бази даних з попередньою обробкою (вставка парольного захисту, перевірки щодо звернення до пристроїв зберігання ключа і ключових дискет, блокування налагоджувальних переривань, перевірка робочої ЕОМ щодо її унікальних характеристик та інше), яка формує код програми, що захищається, і бази даних в стан, що перешкоджає його виконанню на «чужих» машинах.

Контроль цілісності програмного забезпечення проводиться за допомогою зовнішніх засобів (програм контролю цілісності) і за допомогою внутрішніх засобів (вмонтованих в саму програму). Зовнішні засоби здійснюють контроль під час старту системи і кожному запуску програми на виконання. Внутрішні засоби контролюють виконання програм при кожному запуску на виконання і полягають в порівнянні контрольних сум окремих блоків програм з їх еталонними сумами.

Протидію несанкціонованій зміні прикладних і спеціальних програм можна забезпечити різними способами, зокрема методом контролю цілісності базового програмного забезпечення спеціальними програмами.

Під час захисту комерційної інформації користуються всією сукупністю існуючих засобів і систем захисту даних. Проте при їх виборі слід виходити з порівняльної оцінки важливості інформації, її захисту, а також збитку, який може нанести її втрата.

З перерахованих засобів захисту найбільш надійними і ефективними є системи і засоби, побудовані на базі криптографічних методів.

Слід зазначити, що без належної організаційної підтримки програмно-технічних засобів захисту інформації від несанкціонованого доступу і точного виконання, передбачених проектною документацією, процедур в належній мірі не вирішити проблему забезпечення безпеки інформації, якими б ці програмно-технічні засоби не були.

Створення базової системи захисту інформації в ІС ґрунтується на таких принципах:

1. Комплексний підхід до побудови системи захисту при провідній ролі організаційних заходів. Він означає оптимальне поєднання програмних апаратних засобів і організаційних заходів захисту, підтверджене практикою створення вітчизняних і зарубіжних систем захисту.
2. Розділення і мінімізація повноважень щодо доступу до інформації і процедур обробки. Користувачам надається мінімум певних повноважень, достатніх для успішного виконання ними своїх службових обов'язків, з погляду автоматизованої обробки доступної їм конфіденційної інформації.
3. Повнота контролю і реєстрації спроб несанкціонованого доступу, тобто необхідність точного встановлення ідентичності кожного користувача і протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації в ІС без її попередньої реєстрації.
4. Забезпечення надійності системи захисту, тобто неможливість зниження її рівня під час виникнення в системі збоїв, відмов, навмисних дій порушника або ненавмисних помилок користувачів і обслуговуючого персоналу.
5. Забезпечення контролю за функціонуванням системи захисту, тобто створення засобів і методів контролю працездатності механізмів захисту.
6. “Прозорість” системи захисту інформації для загального, прикладного програмного забезпечення і користувачів ІС.
7. Економічна доцільність використання системи захисту. Він виражається в тому, що вартість розробки і експлуатації систем захисту інформації має бути менше за вартість можливого збитку, що наноситься об'єкту у разі розробки і експлуатації ІС без системи захисту інформації.