Інформаційні технології

УДК 007.629.735 **doi: 10.26906/SUNZ.2024.1.038**

А. Н. Аль-Амморі, М. М. Дехтяр, Р. М. Іщенко, А. Є. Клочан

Національний транспортний університет, Київ, Україна

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. Розглядаються загальні питання організації методів і засобів захисту інформації. Розглянуто різні визначення загальнонаукового поняття "інформація", з точки зору різних вчених, дослідників, і залежно від галузі людської діяльності. Розглянуто види представлення інформації та її окремі властивості, стосовно комп'ютерного опрацювання даних. Розглянуто фундаментальні поняття та визначення з області інформаційної безпеки систем. Наведено історичні етапи розвитку засобів захисту інформації, дано класифікацію методів захисту інформації, досліджено основні напрямки їх використання. Розглянуто класифікацію комп'ютерних вірусів за основними їхніми ознаками, а також завдання, які розв'язують антивірусні засоби. Окремо розглянуто криптографічні методи захисту інформації та загальну технологію шифрування.

Ключові слова: інформація, інформаційна безпека, конфіденційність, цілісність, доступність.

Вступ

Протягом усього свого існування людство отримувало нові знання про навколишній світ. Саме нові дані, отримані в процесі пізнання або навчання, називається інформацією. Інформація (лат. informatio - роз'яснення, виклад), першопочатково - відомості, які люди передають усно, письмово або в інший спосіб за допомогою умовних сигналів, технічних засобів тощо. Із середини 20-го століття інформація є загальнонауковим поняттям, що включає: відомості, що передаються між людьми, людиною й автоматом, автоматом і автоматом; сигнали в тваринному і рослинному світі; ознаки, що передаються від клітини до клітини, від організму до організму тощо.

Сучасне наукове уявлення про інформацію дуже точно сформулював Норберт Вінер, "батько" кібернетики: Інформація - це позначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього та пристосування до нього наших почуттів. Відоме також інше його визначення цього поняття: "Інформація є інформація, а не матерія і не енергія". Тим самим Н. Вінер відмовився від формулювання поняття інформації, вважаючи, що воно споріднене з такими категоріями, як рух, життя, свідомість. Добре відоме визначення академіка В.М. Глушкова: "Інформація в найзагальнішому її розумінні являє собою міру неоднорідності розподілу матерії та енергії в просторі та в часі, міру змін, якими супроводжуються всі процеси, що відбуваються у світі. ... Інформацію несуть у собі не тільки поцятковані буквами аркуші книги або людська мова, а й сонячне світло, складки гірського хребта, шум водоспаду, шелест листя". Уявлення про інформацію, що ґрунтуються на статистичній теорії передавання сигналів К. Шеннона, привели до такого визначення у Webster's New World Dictionary of Computer Terms: "Інформація - це дані, які обробляються комп'ютером і можуть бути виведені у формі, зручній для користувача". Визначень інформації існує безліч, причому академік М. М. Моїсеєв навіть вважав, що з огляду на широту цього поняття немає і не може бути суворого і досить універсального визначення інформації. Водночас формулювання терміна "інформація", хоча б у загальному вигляді, необхідне для розв'язання як теоретичних, так і практичних завдань сучасної науки і техніки. Багато в чому визначення інформації залежить від галузі людської діяльності:

- у *побутовому* сенсі під інформацією розуміють будь-які дані або відомості, які когось цікавлять. Наприклад, повідомлення про якісь події, про чиюсь діяльність тощо;

- у *техніці* під інформацією розуміють повідомлення, що передаються у формі знаків або сигналів (у цьому разі є джерело повідомлень, одержувач (приймач) повідомлень, канал зв'язку);

- у кібернетиці під інформацією розуміють ту частину знань, яку використовують для орієнтування, активної дії, управління, тобто з метою збереження, вдосконалення, розвитку системи.

Стосовно *комп'ютерного опрацювання* даних, під інформацією розуміють деяку послідовність символічних позначень (літер, цифр, звуків, графіків, малюнків тощо), яка має смислове навантаження та подана у зрозумілому комп'ютеру вигляді. Фізично інформація в комп'ютері записується і передається у вигляді електричних сигналів. Найзагальніше розуміння терміна "інформація" полягає в тому, що інформація - це відображення розмаїття в існуючому світі. Важливо пам'ятати під час вивчення цього терміна, що жодне з наведених трактувань не може вважатися визначенням. Інформація може існувати у вигляді: тексту, малюнків, фотографій, креслень; світлових або звукових сигналів; радіохвиль; електричних і нервових імпульсів; магнітних записів; жестів і міміки; запахів і смакових відчуттів; хромосом, за посередництвом яких передаються у спадок ознаки і властивості організмів, тощо. Людина сприймає за допомогою органів чуття таку інформацію:

- *візуальну* (сприйняття зорових образів, розрізнення кольорів тощо) – за допомогою зору (90%);

- *звукову* (сприйняття музики, мови, сигналів, шуму тощо) - за допомогою слуху;

- *нюхову* (сприйняття запахів) – за допомогою нюху;

- *смакову* (сприйняття за допомогою смакових рецепторів язика) – за допомогою смаку;

- *тактильну* (за допомогою шкірного покриву сприйняття інформації про температуру, якість предметів тощо) – за допомогою дотику.

Властивості інформації:

- *релевантність* - здатність інформації відповідати потребам (запитам) споживача;

- *повнота* - властивість інформації вичерпно (для даного споживача) характеризувати відображуваний об'єкт або процес;

- *своєчасність* - здатність інформації відповідати потребам у потрібний момент часу;

- *достовірність* - властивість інформації не мати прихованих помилок. Достовірна інформація з часом може стати недостовірною, якщо застаріє і перестане відображати справжній стан справ;

- *доступність* - можливість отримання інформації даним споживачем;

- *захищеність* - властивість, що характеризує неможливість несанкціонованого використання або зміни інформації;

- *ергономічність* - властивість, що характеризує зручність форми або обсягу інформації з точки зору даного споживача.

Основна частина

Всупереч поширеній думці звичайні факти самі по собі ні про що не говорять - вони набувають значення порівняно з іншими фактами. Якщо якісь відомості не несуть для нас смислового навантаження або ж вони не нові для нас, то такий факт залишиться для нас лише фактом. Щодня ми дізнаємося масу нової інформації, потрібної і не дуже. Більшу її частину ми, природно, дізнаємося з Інтернету. Дані та відомості про якісь об'єкти, що перебувають у вільному доступі, належать усім без винятку. Крім того, в Інтернеті люди часто передають один одному величезну кількість особистої інформації. Тому наше суспільство часто називають "інформаційним", адже людство в буквальному сенсі стало залежати від тієї інформації, якою воно володіє.

У сучасному світі інформація являє собою певну для людини цінність. Як і будь-яку іншу цінність, інформацію варто захищати від її неправомірного спотворення або несанкціонованого доступу до неї. Багато користувачів залишилися б незадоволеними, якби інформація особистого характеру, якою вони обмінюються в різних соціальних мережах, перебувала в загальному користуванні. Тому, захист даних від несанкціонованого доступу є одним із пріоритетних завдань під час проектування будь-якої інформаційної системи. Але як правильно захистити інформацію? І чи існує абсолютний захист інформації? Саме ці питання будуть розглянуті в роботі.

Черговий етап технологічної революції, що відбувається нині у світі, спричиняє серйозні зміни в економіці, соціальній структурі суспільства. Масове застосування нових технологічних засобів, на основі яких здійснюється інформатизація, стирає геополітичні кордони, змінює спосіб життя мільйонів людей. Водночас інформаційна сфера стає не тільки однією з найважливіших сфер міжнародного співробітництва, а й об'єктом суперництва.

Нині більшість керівників підприємств і організацій вживають заходів щодо "захисту й оборони" важливої для них інформації. Однак практика показує, що ці дії не завжди мають системний характер. Здебільшого вони спрямовані на ліквідацію тільки окремих загроз, залишаючи проломи в обороні.

На жаль, в Україні до теперішнього часу відсутня єдина система безпеки підприємництва. Тому керівництву будь-якої організації доводиться самостійно вирішувати складне завдання забезпечення своєї економічної та інформаційної безпеки з оптимальними фінансовими витратами, але на необхідному рівні захищеності. Кожне підприємство й організація змушені постійно вести конкурентну боротьбу за своє існування, за прибуткове ведення справ, за своє добре ім'я в умовах становлення ринкової економіки. Успіх виробничої та підприємницької діяльності значною мірою залежить від уміння розпоряджатися таким найцінніш товаром, як інформація. Тому в умовах посилення конкуренції успіх підприємництва, гарантія отримання прибутку дедалі більшою мірою залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і конкретну технологію. Саме поняття "безпека" набуває розширеного змісту, воно охоплює питання інформаційно-комерційної, юридичної та фізичної безпеки, розв'язання яких потребує особливої уваги у зв'язку зі зростаючою роллю інформації в житті суспільства. Розглянемо фундаментальні поняття та визначення з галузі інформаційної безпеки та надійності систем [1– 3]:

Інформація - відомості (дані) про внутрішній і навколишній світ, події, процеси, явища тощо, які сприймаються і передаються людьми або технічними пристроями.

Інформаційна (інформаційно-обчислювальна) система - організаційно впорядкована сукупність документів, технічних засобів та інформаційних технологій, що реалізує інформаційні (інформаційно-обчислювальні) процеси.

Інформаційні процеси - процеси збирання, накопичення, зберігання, опрацювання (перероблення), передавання та використання інформації.

Інформаційні ресурси - окремі документи або масиви документів в інформаційних системах.

Доступ - спеціальний тип взаємодії між об'єктом і суб'єктом, у результаті якого створюється потік інформації від одного до іншого.

Несанкціонований доступ (НСД) - доступ до інформації, пристроїв її зберігання та оброблення, а також до каналів передавання, який реалізують без відома (санкції) власника, порушуючи тим самим встановлені правила доступу.

Об'єкт - пасивний компонент системи, що зберігає, переробляє, передає або приймає інформацію; приклади об'єктів: сторінки, файли, папки, директорії, комп'ютерні програми, пристрої (монітори, диски, принтери тощо).

Суб'єкт - активний компонент системи, який може ініціювати потік інформації; приклади суб'єктів: користувач, процес або пристрій.

Безпека ІВС - властивість системи, що виражається у здатності системи протидіяти спробам неса-

нкціонованого доступу або заподіяння шкоди власникам і користувачам системи за різних навмисних і ненавмисних впливів на неї.

Захист інформації - організаційні, правові, програмно-технічні та інші заходи щодо запобігання загрозам інформаційній безпеці та усунення їх наслідків.

Атака - спроба несанкціонованого подолання захисту системи.

Інформаційна безпека (ІБ) систем - властивість інформаційної системи або реалізованого в ній процесу, що характеризує здатність забезпечити необхідний рівень свого захисту.

Інше визначення:

Інформаційна безпека - усі аспекти, пов'язані з визначенням, досягненням і підтриманням конфіденційності, цілісності, доступності інформації або засобів її обробки:

конфіденційність (confidentiality) - стан інформації, за якого доступ до неї здійснюють тільки суб'єкти, що мають на неї право;

цілісність (integrity) - уникнення несанкціонованої модифікації інформації;

доступність (availability) - уникнення тимчасового або постійного приховування інформації від користувачів, які отримали права доступу.

Цінність інформації визначається ступенем її корисності для власника.

Ідентифікація - процес розпізнавання певних компонентів системи (об'єктів або суб'єктів) за допомогою унікальних ідентифікаторів.

Автентифікація - перевірка ідентифікації користувача або іншого компонента ІС для ухвалення рішення про дозвіл доступу до ресурсів системи.

Надійність системи - характеристика здатності програмного, апаратного, апаратно-програмного засобу виконати за певних умов необхідні функції протягом певного періоду часу за певних умов.

Достовірність роботи системи (пристрою) - властивість, що характеризує істинність кінцевого (вихідного) результату роботи (виконання програми), яка визначається здатністю засобів контролю фіксувати правильність або помилковість роботи.

Помилка пристрою - неправильне значення сигналу (біта - у цифровому пристрої) на зовнішніх виходах пристрою або окремого його вузла, спричинене технічною несправністю, або перешкодами, що впливають на нього (навмисними чи ненавмисними), або іншим способом.

Помилка програми - проявляється в невідповідному реальному (необхідному) проміжному або кінцевому значенню (результату) внаслідок неправильно запрограмованого алгоритму або програми.

Достовірність інформації визначається достатньою для володільця точністю відображати об'єкти і процеси навколишнього світу в певних часових і просторових рамках. Інформація, що спотворено представляє дійсність, може завдати власнику значної матеріальної та моральної шкоди. Якщо інформація спотворена навмисно, то її називають дезінформацією. Своєчасність інформації, тобто відповідність цінності та достовірності певному часовому періоду. Ця властивість визначається виразом

$$C(t) = C_0 e^{-2,3t/\tau},$$

де C_0 – цінність інформації в момент її виникнення; t – час від моменту виникнення інформації до моменту визначення її вартості; τ – час від моменту виникнення інформації до моменту її застарівання. Історичні етапи розвитку засобів захисту інформації представлено табл. 1 [4–6].

Таблиця 1 – **Історичні етапи розвитку засобів захисту інформації**

Етапи розвитку засобів ІБ	Коротка характеристика етапу
I етап - приблизно до 1915/16 року	характеризується використанням засобів інформаційних комунікацій, що природно виникали. Основне завдання інформаційної безпеки - захист відомостей про події, факти, майно тощо.
II етап – починаючи з 1916 року	пов'язаний із початком використання технічних засобів електро- і радіозв'язку. Характеризується застосуванням завадостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).
III етап – починаючи з 1935 року	пов'язаний із появою радіолокаційних і гідроакустичних засобів. Забезпечення інформаційної безпеки ґрунтувалося на поєднанні організаційних і технічних заходів, спрямованих на підвищення захищеності радіолокаційних засобів від впливу на їхні приймальні пристрої активних і пасивних перешкод.
IV етап – починаючи з 1946 року	пов'язаний із винаходом і впровадженням у практичну діяльність електронно-обчислювальних машин (комп'ютерів). Еру появи комп'ютерної техніки пов'язують із розробкою в Пенсільванському університеті (США) ЕОМ EN IAC (Electronic Numerical Integrator And Computer (Calculator)). Завдання інформаційної безпеки розв'язували здебільшого методами та способами обмеження фізичного доступу до обладнання засобів збирання, перероблення та передавання інформації.
V етап – починаючи з 1964/65 років	обумовлений створенням та розвитком локальних інформаційно-комунікаційних мереж. Завдання безпеки вирішувалися в основному методами та способами фізичного захисту коштів шляхом адміністрування та управління доступом до мережних ресурсів.
VI етап - починаючи з 1973 року	пов'язаний із використанням мобільних комунікаційних пристроїв із широким спектром завдань. У цей період створено відомі зараз у всьому світі фірми Microsoft (Білл Гейтс і Пол Ален) і Apple (Стів Джобс і Стефан Возняк). Утворилися співтовариства людей - хакерів, які ставлять собі за мету завдання шкоди інформаційній безпеці окремих користувачів, організацій і цілих країн. Формується інформаційне право - нова галузь міжнародної правової системи.
VII етап – починаючи з 1985 року	пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Передбачає комплексне використання заходів і засобів захисту.
VIII етап – приблизно з кінця XX - початку XXI ст.	пов'язаний із повсюдним використанням надмобільних комунікаційних пристроїв із широким спектром завдань і глобальним охопленням у просторі та часі, що забезпечується космічними інформаційно-комунікаційними системами. Характеризується "широким переходом на цифру". Передбачає комплексне використання заходів і засобів захисту.

Комп'ютерні злочини надзвичайно багатогранні та складні явища. Об'єктами таких злочинних посягань можуть бути самі технічні засоби (комп'ютери та периферія) як матеріальні об'єкти або ж програмне забезпечення та бази даних, для яких технічні засоби є оточенням; комп'ютер може виступати як предмет посягань або як інструмент.

Види комп'ютерних злочинів надзвичайно різноманітні. Це і несанкціонований доступ до інформації, що зберігається в комп'ютері, і введення в програмне забезпечення "логічних бомб", що спрацьовують при виконанні певних умов і частково або повністю виводять з ладу комп'ютерну систему, і розробка, і розповсюдження комп'ютерних вірусів, і розкрадання комп'ютерної інформації. Комп'ютерний злочин може статися також через недбалість у розробці, виготовленні та експлуатації програмно-обчислювальних комплексів або через підробку комп'ютерної інформації [7, 8].

Серед усього набору методів захисту інформації виділяють перераховані нижче (рис. 1).

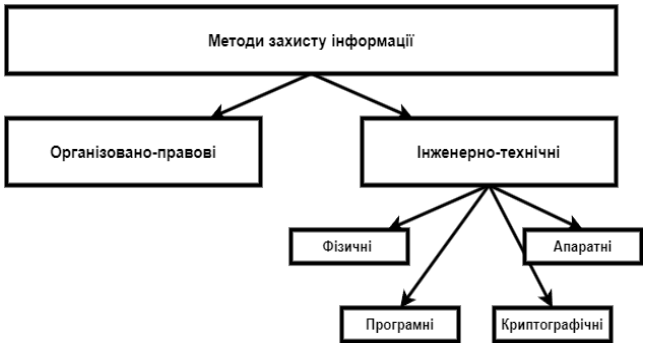

Рис. 1. Класифікація методів захисту інформації в комп'ютерних системах

Методи та засоби організаційно-правового захисту інформації. До методів і засобів організаційного захисту інформації належать організаційно-технічні та організаційно-правові заходи, що проводяться в процесі створення та експлуатації КС для забезпечення захисту інформації. Ці заходи мають проводитися під час будівництва або ремонту приміщень, у яких розміщуватимуться комп'ютери; проєктування системи, монтажу та налагодження її технічних і програмних засобів; випробувань і перевірки працездатності комп'ютерної системи.

Основою проведення організаційних заходів є використання та підготовка законодавчих і нормативних документів у сфері інформаційної безпеки, які на правовому рівні мають регулювати доступ до інформації з боку споживачів.

Методи та засоби інженерно-технічного захисту інформації. Інженерно-технічний захист (ІТЗ) - це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації.

Різноманіття цілей, завдань, об'єктів захисту і заходів, що проводяться, передбачає розгляд деякої системи класифікації засобів за видом, орієнтацією та іншими характеристиками. Наприклад, засоби інженерно-технічного захисту можна розглядати за об'єктами їхнього впливу. У цьому плані вони можуть застосовуватися для захисту людей, матеріальних засобів, фінансів, інформації. Різноманіття класифікаційних характеристик дає змогу розглядати інженерно-технічні засоби за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким чиниться протидія з боку служби безпеки.

За функціональним призначенням засоби інженерно-технічного захисту поділяються на такі групи:

1) *фізичні засоби*, що включають різні засоби і споруди, які перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту і до матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних засобів, фінансів та інформації від протиправних впливів;

2) *апаратні засоби* - прилади, пристрої, пристосування та інші технічні рішення, що використовуються в інтересах захисту інформації. У практиці діяльності підприємства знаходить широке застосування найрізноманітніша апаратура, починаючи з телефонного апарата до досконалих автоматизованих систем, що забезпечують виробничу діяльність. Основне завдання апаратних засобів - забезпечення стійкого захисту інформації від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення виробничої діяльності;

3) *програмні засоби*, що охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різного призначення та засобах обробки (збирання, накопичення, зберігання, обробка та передача) даних;

4) криптографічні засоби - це спеціальні математичні та алгоритмічні засоби захисту інформації, яку передають системами і мережами зв'язку, зберігають і обробляють на ЕОМ із використанням різноманітних методів шифрування.

Фізичні методи та засоби захисту інформації. Фізичні засоби захисту - це різноманітні пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників. До фізичних засобів належать механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для перешкоджання несанкціонованому доступу (входу, виходу), пронесенню (виносу) засобів і матеріалів, та інших можливих видів злочинних дій.

Ці засоби застосовуються для вирішення таких завдань:

1) охорона території підприємства і спостереження за нею;

2) охорона будівель, внутрішніх приміщень і контроль за ними;

3) охорона обладнання, продукції, фінансів та інформації;

4) здійснення контрольованого доступу в будівлі та приміщення.

Усі фізичні засоби захисту об'єктів можна поділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз. Охоронна сигналізація та охоронне телебачення, наприклад,

належать до засобів виявлення загроз; паркани навколо об'єктів - це засоби запобігання несанкціонованому проникненню на територію, а посилені двері, стіни, стелі, решітки на вікнах та інші заходи слугують захистом і від проникнення, і від інших злочинних дій (підслуховування, обстріл, кидання гранат і вибухових пакетів тощо). Засоби пожежогасіння належать до систем ліквідації загроз.

Апаратні методи та засоби захисту інформації. До апаратних засобів захисту інформації належать найрізноманітніші за принципом дії, пристроєм і можливостями технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації.

Апаратні засоби захисту інформації застосовуються для вирішення таких завдань:

1) проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;

2) виявлення каналів витоку інформації на різних об'єктах і в приміщеннях;

3) локалізація каналів витоку інформації;

4) пошук і виявлення засобів промислового шпигунства;

5) протидія несанкціонованому доступу до джерел конфіденційної інформації та іншим діям.

Програмні методи та засоби захисту інформації

Системи захисту комп'ютера від чужого вторгнення вельми різноманітні і класифікуються, як:

1) засоби власного захисту, передбачені загальним програмним забезпеченням;

2) засоби захисту в складі обчислювальної системи;

3) засоби захисту із запитом інформації;

4) засоби активного захисту;

5) засоби пасивного захисту та інші.

Основні напрями використання програмного захисту інформації. Можна виокремити такі напрями використання програм для забезпечення безпеки конфіденційної інформації, зокрема такі:

1) захист інформації від несанкціонованого доступу;

2) захист інформації від копіювання;

3) захист програм від копіювання;

4) захист програм від вірусів;

5) захист інформації від вірусів;

6) програмний захист каналів зв'язку.

За кожним із зазначених напрямів є достатня кількість якісних, розроблених професійними організаціями і розповсюджуваних на ринках програмних продуктів.

Програмні засоби захисту мають такі різновиди спеціальних програм:

1) ідентифікації технічних засобів, файлів та автентифікації користувачів;

2) реєстрації та контролю роботи технічних засобів і користувачів;

3) обслуговування режимів обробки інформації обмеженого користування;

4) захисту операційних засобів ЕОМ і прикладних програм користувачів;

5) знищення інформації в захисні пристрої після використання;

6) сигналізують порушення використання ресурсів;

7) допоміжних програм захисту різного призначення.

Захист інформації від несанкціонованого доступу

Для захисту від чужого вторгнення обов'язково передбачаються певні заходи безпеки. Основні функції, які мають здійснюватися програмними засобами, це:

1) ідентифікація суб'єктів та об'єктів;

2) розмежування (іноді й повна ізоляція) доступу до обчислювальних ресурсів та інформації;

3) контроль і реєстрація дій з інформацією та програмами.

Найпоширенішим методом ідентифікації є парольна ідентифікація. Однак практика показує, що парольний захист даних є слабкою ланкою, оскільки пароль можна підслухати або підглянути, перехопити або просто розгадати.

Захист від копіювання. Засоби захисту від копіювання запобігають використанню крадених копій програмного забезпечення і є нині єдиним надійним засобом, який як захищає авторське право програмістів-розробників, так і стимулює розвиток ринку. Під засобами захисту від копіювання розуміють засоби, що забезпечують виконання програмою своїх функцій тільки в разі розпізнання деякого унікального елемента, що не копіюється. Таким елементом (званим ключовим) може бути дискета, певна частина комп'ютера або спеціальний пристрій, який під'єднують до персонального комп'ютера.

Захист від копіювання реалізується виконанням низки функцій, які є загальними для всіх систем захисту:

1) ідентифікація середовища, з якого запускатиметься програма (дискета або ПК);

2) аутентифікація середовища, з якого запущено програму;

3) реакція на запуск із несанкціонованого середовища;

4) реєстрація санкціонованого копіювання;

5) протидія вивченню алгоритмів роботи системи.

6) захист програм і даних від комп'ютерних вірусів

Шкідницькі програми і, насамперед, віруси становлять дуже серйозну небезпеку при зберіганні на ПЕОМ конфіденційної інформації. Недооцінка цієї небезпеки може мати серйозні наслідки для інформації користувачів. Знання механізмів дії вірусів, методів і засобів боротьби з ними дає змогу ефективно організувати протидію вірусам, звести до мінімуму ймовірність зараження і втрат від їхнього впливу.

"Комп'ютерні віруси" - це невеликі виконувані або інтерпретовані програми, що мають властивість розповсюдження і самовідтворення (реплікації) в комп'ютерній системі. Віруси можуть виконувати зміну або знищення програмного забезпечення або

даних, що зберігаються в ПЕОМ. У процесі поширення віруси можуть себе модифікувати.

Класифікація комп'ютерних вірусів. Нині у світі налічується понад 40 тисяч тільки зареєстрованих комп'ютерних вірусів. Оскільки переважна більшість сучасних шкідницьких програм мають здатність до саморозмноження, то часто їх відносять до комп'ютерних вірусів.

Усі комп'ютерні віруси можуть бути класифіковані за такими ознаками:

- за середовищем існування вірусу,
- за способом зараження середовища проживання,
- за деструктивними можливостями,
- за особливостями алгоритму вірусу.

Масове поширення вірусів, серйозність наслідків їхнього впливу на ресурси комп'ютерів спричинили необхідність розроблення та використання спеціальних антивірусних засобів і методів їхнього застосування. Антивірусні засоби застосовуються для вирішення таких завдань:

- виявлення вірусів у КС,
- блокування роботи програм-вірусів,
- усунення наслідків впливу вірусів.

Виявлення вірусів бажано здійснювати на стадії їх впровадження або, принаймні, до початку здійснення деструктивних функцій вірусів. Необхідно зазначити, що не існує антивірусних засобів, які гарантують виявлення всіх можливих вірусів.

У разі виявлення вірусу необхідно одразу ж припинити роботу програми-вірусу, щоб мінімізувати збитки від його впливу на систему.

Усунення наслідків впливу вірусів ведеться у двох напрямках:

- видалення вірусів,
- відновлення (за необхідності) файлів, областей пам'яті.

Для боротьби з вірусами використовуються програмні та апаратно-програмні засоби, які застосовуються в певній послідовності та комбінації, утворюючи методи боротьби з вірусами.

Найнадійнішим методом захисту від вірусів є використання апаратно-програмних антивірусних засобів. Нині для захисту ПК використовуються спеціальні контролери та їх програмне забезпечення. Контролер встановлюється в роз'єм розширення і має доступ до загальної шини. Це дає йому змогу контролювати всі звернення до дискової системи. У програмному забезпеченні контролера запам'ятовуються області на дисках, зміна яких у звичайних режимах роботи не допускається. Таким чином, можна встановити захист на зміну головного завантажувального запису, завантажувальних секторів, файлів конфігурації, виконуваних файлів тощо.

У разі виконання заборонених дій будь-якою програмою контролер видає відповідне повідомлення користувачеві і блокує роботу ПК.

Апаратно-програмні антивірусні засоби мають низку переваг перед програмними:

- працюють постійно;
- виявляють усі віруси, незалежно від механізму їхньої дії;
- блокують недозволені дії, які є результатом роботи вірусу або некваліфікованого користувача.

Недолік у цих засобів один - залежність від апаратних засобів ПЕОМ. Зміна останніх веде до необхідності заміни контролера.

Сучасні програмні антивірусні засоби можуть здійснювати комплексну перевірку комп'ютера на предмет виявлення комп'ютерних вірусів. Для цього використовуються такі антивірусні програми як - Kaspersky Anti-Virus (AVP), Norton Antivirus, Dr. Web, Symantec Antivirus. Усі вони мають антивірусні бази, які періодично оновлюються.

Криптографічні методи та засоби захисту інформації. Криптографія як засіб захисту (закриття) інформації набуває дедалі важливішого значення у світі комерційної діяльності.

Криптографія має досить давню історію. Спочатку вона застосовувалася головним чином у сфері військового і дипломатичного зв'язку. Тепер вона необхідна у виробничій і комерційній діяльності. Якщо врахувати, що сьогодні каналами шифрованого зв'язку тільки у нас у країні передають сотні мільйонів повідомлень, телефонних переговорів, величезні обсяги комп'ютерних і телеметричних даних, і все це не для чужих очей і вух, стає зрозумілим: збереження таємниці цієї інформації тут украй необхідне.

Криптографія охоплює кілька розділів сучасної математики, а також спеціальні галузі фізики, радіоелектроніки, зв'язку та деяких інших суміжних галузей. Її завданням є перетворення математичними методами переданого каналами зв'язку секретного повідомлення, телефонної розмови або комп'ютерних даних таким чином, що вони стають абсолютно незрозумілими для сторонніх осіб. Тобто криптографія повинна забезпечити такий захист секретної (або будь-якої іншої) інформації, що навіть у разі її перехоплення сторонніми особами та обробки будь-якими способами з використанням найшвидкодіючіших ЕОМ і останніх досягнень науки і техніки, вона не має бути дешифрована протягом кількох десятків років. Для такого перетворення інформації використовують різні шифрувальні засоби - такі, як засоби шифрування документів, зокрема й портативного виконання, засоби шифрування мовлення (телефонних і радіопереговорів), телеграфних повідомлень і передавання даних.

Загальна технологія шифрування. Початкова інформація, яка передається каналами зв'язку, може являти собою мову, дані, відеосигнали, називається незашифрованими повідомленнями Р.

У пристрої шифрування повідомлення Р шифрується (перетворюється на повідомлення С) і передається "незакритим" каналом зв'язку. На приймальній стороні повідомлення С дешифрується для відновлення вихідного значення повідомлення Р. Параметр, який може бути застосований для вилучення окремої інформації, називається ключем. Якщо в процесі обміну інформацією для шифрування і читання використовувати один той самий ключ, то такий криптографічний процес називається симетричним. Його основним недоліком є те, що перш

ніж почати обмін інформацією, потрібно виконати передачу ключа, а для цього необхідний захищений зв'язок.

Нині під час обміну даними каналами зв'язку використовується несиметричне криптографічне шифрування, засноване на використанні двох ключів. Це нові криптографічні алгоритми з відкритим ключем, засновані на використанні ключів двох типів: секретного (закритого) і відкритого.

У криптографії з відкритим ключем є принаймні два ключі, один з яких неможливо обчислити з іншого. Якщо ключ розшифрування обчислювальними методами неможливо отримати з ключа зашифрування, то секретність інформації, зашифрованої за допомогою несекретного (відкритого) ключа, буде забезпечена. Однак цей ключ має бути захищений від підміни або модифікації. Ключ розшифрування також має бути секретним і захищений від підміни або модифікації.

Якщо, навпаки, обчислювальними методами неможливо отримати ключ зашифрування з ключа розшифрування, то ключ розшифрування може бути не секретним.

Ключі влаштовані таким чином, що повідомлення, зашифроване однією половинкою, можна розшифрувати тільки іншою половинкою. Створивши пару ключів, компанія широко поширює відкритий (публічний) ключ і надійно охороняє закритий (особистий) ключ.

Захист публічним ключем не є абсолютно надійним. Вивчивши алгоритм його побудови, можна реконструювати закритий ключ. Однак знання алгоритму ще не означає можливість провести реконструкцію ключа в розумно прийнятні терміни. Виходячи з цього, формується принцип достатності захисту інформації: захист інформації прийнято вважати достатнім, якщо витрати на його подолання перевищують очікувану вартість самої інформації. Цим принципом керуються під час несиметричного шифрування даних.

Поділ функцій зашифрування і розшифрування за допомогою поділу на дві частини додаткової інформації, необхідної для виконання операцій, є тією цінною ідеєю, яка лежить в основі криптографії з відкритим ключем.

Криптографічному захисту фахівці приділяють особливу увагу, вважаючи його найнадійнішим, а для інформації, що передається по лінії зв'язку великої протяжності, – єдиним засобом захисту від розкрадань.

Висновки

1. Поняття інформації ємне, багатогранне, а її визначення багато в чому залежить від галузі людської діяльності.
2. Інформація, як об'єктивне відображення реальності, може існувати в різних формах і мати певні властивості, водночас людина може сприймати за допомогою органів чуття 5 її видів.
3. Поняття інформаційної безпеки є ключовою умовою успіху виробничої та підприємницької діяльності, і включає в себе питання інформаційно-комерційної, юридичної та фізичної безпеки.
4. Класифікація методів захисту інформації включає в себе організаційно-правові, інженерно-технічні методи, які, своєю чергою, складаються з фізичних, апаратних, програмних і криптографічних методів.

СПИСОК ЛІТЕРАТУРИ

1. Безруков, В.В. Теорія інформації / В.В. Безруков, В.Я. Кізяков, В.І. Профатілов. – Д.: ДДТУЗТ, 2001. – 110 с.
2. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування: Підручник.- К.:Вища школа, 2011. — 255 с.
3. Тулякова Н. О. Теорія інформації: Навчальний посібник. - Суми: Вид-во СумДУ, 2008.- 212 с.
4. Кулик А.Я., Кривогубченко С.Г. Теорія інформації і кодування / Навч. посібник. – Вінниця: ВНТУ, 2008. 145 с.
5. Ali Al-Ammouri. Development of a mathematical model of reliable structures of information-control systems / Ali Al-Ammouri, Iryna Lebid, Marina Dekhtiar, Ievgenii Lebid, Hasan Al-Ammori // Eastern-European Journal of Enterprise Technologies. – 2022. – Vol. 5/9, Issue (119).– P. 68–78. DOI: https://doi.org/10.15587/1729-4061.2022.265953.
6. Інформаційні системи та мережі: навчальний посібник. / Аль-Амморі. А.Н, Лясковський В.П., Попова Л.С., Тимченко О.П, Полєва Н.М. – К-НТУ-2021, 194с.
7. Подлевський Б. М. Теорія інформації : підручник / Б. М. Подлевський, Р. Є. Рикалюк. – Львів: Видавничий центр ЛНУ ім. І. Франка, 2016. – 342 с.
8. Методологія і технології захисту інформації: навчальний посібник / А.Н. Аль-Амморі, Н.М. Наумова, П.В. Дяченко, Р.М. Іщенко, М.М. Дехтяр, А.Є. Клочан; НТУ. – Київ: НТУ, 2020. – 147с.

Received (Надійшла) 22.11.2023
Accepted for publication (Прийнята до друку) 10.01.2024

Methods and means of protecting information

A. Al-Ammouri, M. Dekhtyar, R. Ishchenko, E. Klochan

Abstract. The article discusses general issues of organizing methods and means of information protection. Various definitions of the general scientific concept of "information" are considered, from the point of view of various scientists, researchers, and depending on the branch of human activity. The types of information presentation and its individual properties in relation to computer data processing are considered. The fundamental concepts and definitions from the field of information security of systems are considered. The historical stages in the development of information security means are given, the classification of information security methods is given, the main directions of their use are investigated. The classification of computer viruses by their main features, as well as the tasks solved by antivirus tools, are considered. Cryptographic methods of information protection and general encryption technology are considered separately.

Keywords: information, information security, confidentiality, integrity, availability.