УДК 343.534:004.56 (045)

О. І. Мотлях, кандидат юридичних наук, доцент,
завідувач кафедри кримінального права та процесу
Юридичного інституту «Інститут повітряного і космічного права»
Національного авіаційного університету

БЕЗПЕКА КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ДАНИХ: РЕАЛІЇ СЬОГОДЕННЯ ТА ПЕРСПЕКТИВИ

Юридичний інститут «Інститут повітряного і космічного права» НАУ

У статті розглядаються питання, пов'язані з забезпеченням безпеки комп'ютерної інформації у процесі її обробки та передачі електронних даних, а також несанкціоновані дії злочинців з використання ЕОМ (комп'ютерів) комп'ютерних систем і систем електрозв'язку.

Ключові слова: комп'ютерна інформація, електронні данні, комп'ютерні системи, ЕОМ, системи електрозв'язку.

Третє тисячоліття, за висловленнями фахівців-дослідників сфери електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, період повного розквіту комп'ютеризації на нашій планеті. Більш як піввіковий термін, від створення перших ЕОМ до сучасності, свідчить про надзвичайно швидкий хід руху комп'ютерних технологій, впровадження їх практично в усі сфери людської життєдіяльності [4, с.12]. Комп'ютеризація стала невід'ємною частиною нашого буття. Але разом з тим вона перетворилася на камінь спотикання саме, з точки зору інформаційної безпеки. Несанкціоновані дії «білокомірцевих злочинців» з конфіденційною, а також таємною електронною машинною інформацією, що є приватною власністю фізичних, юридичних осіб чи держави, як результат приводять до: викрадення комп'ютерних даних, їх перекручення, блокування, маніпуляції, порушення її маршрутизації чи знищення такої. Зазначені злочинні дії осіб в кінцевому результаті спричиняють небажаних, а також шкідливих наслідків (збитків): витоків ЕОМ (комп'ютерної) інформації; приведення її у непридатний стан; послаблення, виснаження та завдання матеріальної шкоди її законним власникам.

Існуючі системи захисту збереження комп'ютерної інформації, технологічно в цілому не можуть охопити весь спектр контролю за доступом до операційних програмних систем, комп'ютерних мереж чи мереж електрозв'язку. Якщо до недавна потенційні користувачі програмних забезпечень приділяли увагу переважно придбанню та оновленню робочих місць найсучаснішими розробками науки та техніки, створюючи виробничому процесу більш швидкого та зручного опрацювання електронних даних, її мобільної передачі іншим адресатам, у тому числі, з метою обміну досвідом спеціалістів різних сфер та галузей, співпраці правоохоронних систем тощо. То нині нагальним питанням є цілісне збереження накопичуваної інформації, її захист від несанкціонованих проникнень різної категорії комп'ютерних зломщиків. Як свідчить зарубіжна практика, провідні державні та приватні установи щорічно витрачають від 20 до 40 % чистого прибутку на придбання оновлених систем захисту програмних продуктів від їх викрадення [7, с.23-25]. Хоч загально відомо, що не існує єдиного досконалого програмного забезпечення, яке на 100% змогло б гарантувати безпечність витоків комп'ютерної інформації, а значить, не виключається можливість бути потенційно пограбованим, навіть і не підозрюючи на те. Саме по собі виникає риторичне запитання: які ж системи захисту все ж таки є діючими, а не лише існуючими, що знижують ймовірність від несанкціонованих дій з боку злочинців, що спеціалізуються у цій сфері, і що вони собою являють?

Перш за все потрібно сказати, що безпека інформаційних даних, які обробляються у ЕОМ (комп'ютерних) системах, та комп'ютерних мережах і мережах електрозв'язку розглядається через дві складові: висока ступінь захисту програмних продуктів та низька.

1. Висока включає в себе ширше поняття, бо охоплює не лише безпеку програмного забезпечення, а й місце територіального розташування будівель, приміщень, кімнат, в яких знаходяться комп'ютерні устаткування. Зокрема здійснює такі заходи:

— постійну охорону території і споруд за допомогою технічних засобів безпеки та відповідного персоналу;

— спеціальне облаштування, екранування приміщень;

— введення адміністратора служби захисту інформації;

систему доступу, допуску та контролю роботи за операційною системою.

Постійна охорона території, де знаходяться засоби комп'ютерної техніки (далі по тексту ЗКТ), це перший чинник при досягненні інформаційної безпеки. Обнесення споруд відповідними спеціальними контролюючими пристроями, які спрацьовують на несанкціоноване перехоплення комп'ютерної інформації, зчитування або заважання операційній системі нормальному, ритмічному функціонуванню. Адже технічних способів викрадення ЕОМ (комп'ютерних) даних існує досить велика чисельність, основні з них:

безпосереднє (активне) перехоплення;

електромагнітне (пасивне);

аудіо і відео перехоплення;

Скориставшись шляхами:

— прямого викрадення, безпосереднього підслуховування та спостереження;

шляхом перехоплення машинної інформації мережевими каналами зв'язку;

шляхом використання різних джерел сигналів у приміщеннях, пов'язаних з функціональним обладнанням за допомогою спеціальних «жучків», «закладок», «таблеток» тощо.

На противагу цьому обширному переліку систем і способів несанкціонованого отримання комп'ютерної інформації протистоять оригінальні розробки безпеки ЗКТ фахівців світової спільноти. А саме: технічного перешкодження відеозапису; застосування приймачів-сканерів, які автоматично реєструють підслуховуючі прилади; приймачів для пошуку радіопередавачів; впровадження рентгенівської та лазерної техніки, спрямування пучків відповідного обладнання лазеру зустрічному пучку перехоплювача машинної (електронної) інформації, зміни тим самим коливань амплітуди в інженерних конструкціях; застосування електромагнітних модуляторів коливань та інше.

Чільне місце відводиться екрануванню споруд, як зовнішнього боку будівельних конструкцій, так і внутрішнього. Захищення тих ділянок приміщення, де ймовірніше за все відбувається перехоплення інформаційних комп'ютерних даних, зокрема: комп'ютерних мереж, мереж електрозв'язку, серверних та переговорних кімнат, електронної пошти та ін. Принцип екранування полягає у спеціальному обнесенні (обгородженні) металом або металевою сіткою ділянок високочутливого діапазону. Інакше електромагнітний фон, що створюється від технічного устаткування перетворюється у своєрідний гучномовець, з якого придатно вилучити комп'ютерну інформацію у процесі її маршрутизації іншим абонентам. Здається особливої мудрості в цьому і немає, але саме практичне застосування екранування приміщення дає ефект послаблення витоків фонового сигналу у мільйони разів. Схоже нововведення було запропоновано ще на прикінці минулого століття однією з провідних англійських фірм, що спеціалізувалася на захисті ЗКТ, програмних продуктів та комп'ютерної інформації «Білліш-Лі», яка пропонувала застосування герметичної в кілька тонн сталевої кабіни наповненої різномагнітнішими фільтрами та хвилегасниками, але у зв'язку зі своїми надзвичайно великими габаритними розмірами не знайшла підтримки у потенційних споживачів ЕОМ (комп'ютерів) [3, с.17-20].

Один з видів модернізованого вигляду екранування приміщень було запропоновано вітчизняними виробниками у співробітництві зі спеціалістами ІЕЗ ім. Е.О. Патона Національної Академії наук України. Фахівці запропонували спеціалізований комплексний захист витоків комп'ютерної інформації шляхом екранування відповідних приміщень з дотриманням запропонованих вимог. Це проце-

дура екранованого тестування технологій зварювання металів будь-якої складності, захист вхідних та вихідних комунікаційних ліній, встановлення екранованих дверей, систем пожежогасіння, заземлення тощо. Розробка пройшла ряд випробувань знайшла своє практичне застосування. Як підтвердження тому Національний банк України зобов'язав усі банківські установи та філії облаштувати серверні приміщення електромагнітними екранами з послабленнями не менше 20 дб. (Нст. НБУ № 216 від 29.08.1997р.) [6, с. 10-12].

Окреме місце у системі захисту комп'ютерної інформації від її несанкціонованого використання є введення адміністратора (служби захисту інформації) та системи доступу, допуску та контролю всього виробничого процесу. Як свідчить зарубіжна практика введення в штатний розпис адміністратора по захисту інформаційних даних у кілька разів знижує ймовірність скоєння комп'ютерних злочинів. Така особа або окремий відділ – це є спеціально підготовлені кадри, професіонали вищого гатунку, які пройшли стажування у відповідних установах, центрах [5, с. 32]. Обов'язками яких, окрім організаційних засобів підтримки та контролю безпеки ЗКТ, є робота з персоналом, зокрема, ознайомлення та навчання відповідних кадрів з організацією та організаційно-технічною діяльністю захисту від стороннього втручання. А також:

визначення для всіх осіб, що мають доступ до ЗКТ категорій допуску до тієї чи іншої комп'ютерної інформації (ведення електронного журналу);

розмежування та групування комп'ютерної інформації за її важливістю, охоронний порядок її збереження та знищення;

проведення регламентних робіт у системі контролю безпеки ЗКТ, захисту інформаційних електронних даних (при потребі із залученням експертів у даній галузі);

– захист апаратних засобів та засобів комп'ютерної техніки від небажаних фізичних впливів на них сторонніх сил;

перекриття каналів можливих витоків машинної (комп'ютерної) інформації через системи наведень, віброакустичних сигналів та побічних електромагнітних випромінювань;

– фізичний захист засобів комп'ютерної техніки [5, с. 37].

2. Низький ступінь захисту – це більш вузько направлений напрямок безпеки витоків комп'ютерної інформації. Він визначається наявністю простого алгоритму обмеження доступу до програмного забезпечення, системи та комп'ютерної мережі чи мережі електрозв'язку. Тобто, застосуванні аутентифікації (перевірка оригіналу) через паролі та коди, ідентифікації (встановлення тотожності особи), системи реєстрації та сертифікації, допуску та протоколювання, проведення аудиту та інше. Наявність істинного добросовісного користувача конфіденційної інформації підтверджується знанням зазначеного у системі допуску пароля, криптографічного ключа, особистого ідентифікаційного номера. Можливого використання особистої магнітної карточки або іншого технічного облаштування аналогічного типу. Ідентифікуванням за біометричними параметрами людини (за голосом, сітчаткою очей, відпечатками папілярних візерунків пальців рук та ін.).

Розкриваючи сутність низького способу захисту від витоків інформації, слід зосередити увагу на найголовнішому аспекті реєстрації та сертифікації ЗКТ, які є первинною ланкою у системі інформаційної безпеки. Реєстрацію потрібно розглядати під двома кутами бачення, тобто:

1) реєстрація та сертифікація технічних комп'ютерних засобів, як система відповідності певним встановленим стандартам;

2) реєстрація, як моніторинговий спосіб контролю за діяльністю всієї операційної системи.

Реєстрація є основою сертифікації. Це певний комплекс організаційно-технічних заходів, які проводяться уповноваженими на те органами, у результаті чого підтверджується, що засоби технічного захисту інформації, у тому числі й комп'ютерної, відповідають стандартам або іншим нормативно-технічним документам з питань безпеки. Це своєрідне тестування всієї системи або окремої її ділянки на придатність характеристик та властивостей технічної забезпеченості через показники випробувань у відповідності до встановлених стандартів безпеки та видача на даний програмний продукт сертифікату якості.

Інший аспект реєстрації, як засіб контролю доступу до операційної системи. Він є ло-

сить ефективним у намірах несанкціонованого проникнення комп'ютерних зломщиків у ЕОМ (комп'ютери), системи та комп'ютерні мережі чи мережі електрозв'язку. Основним завданням реєстрації є виявлення та фіксація різного плану порушень роботи ЗКТ, а також запобігання можливих комп'ютерних загроз своєрідному моніторингу. Функції моніторингу включають у себе контроль за процесами введення та виведення, обробки та знищення машинної інформації. Здійснення сигнального повідомлення про стороннє втручання у роботу комп'ютерних систем з одночасним виведенням на друк відповідної інформації.

Стосовно профілактичних заходів моніторингової системи, то за твердженнями фахівців у сфері, що розглядається, повинні бути створені всі умови, за яких допущення помилок випадкового змінення інформаційних даних не повинно мати місця. А тому:

— програми захисту зареєстрованих первинних даних мають бути відмежовані від передбаченого або випадкового їх змінення сторонніми особами;

втручання у роботу системи реєстрації, внесення змін у машинний запис про первинні дані, має право лише особа, яка наділена відповідними повноваженнями.

Найпоширенішого розповсюдження безпеки доступу до програмного продукту та його комп'ютерної інформації набула аутентифікація шляхом введення паролів та кодів програм. Такі дані заносять в операційні системи або серверні програми безпосередньо самі користувачі ЕОМ (комп'ютерів), систем та комп'ютерних мереж чи мереж електрозв'язку. Це може бути, як набір певних чисел та цифр, так і окремі умовні позначення та дати, які легко запам'ятовуються або асоціативно пов'язані з певною подією тієї чи іншої особи. Кількісний показник, тобто довжина паролю, знаходиться у межах від 4 до 12 цифр. Для безпечності спеціалісти рекомендують не користуватися довгий час одним кодом та паролем, а змінювати його, так як це може призвести до копіювання та розпізнання даного набору позначень сторонньою особою. Максимальний термін дії пароля або коду не повинен перевищувати 30 днів [1, с. 31].

Наступним засобом аутентифікації вважається система з магнітними картками, криптоалгоритмами та їх модифікаціями. Це так звані токени — предмети та улаштування, що зазначають особу оригіналу (добросовісного власника). Користувач набирає свій ідентифікаційний номер, після чого процесор перевіряє набраний номер з тим, що зазначений на магнитній картаці, а заодно і перевіряє справжність самого носія інформації. Рідше, але при допуску до операційної програми такі картки застосовуються і без ідентифікаційного номеру. Дана система має ряд переваг, особливо перед процедурою допуску через протоколювання, що створює ряд операційних навантажень, які ускладнюють весь виробничий процес. Для уникнення способу містифікації, тобто отримання конфіденційної інформації особою, яка є недобросовісним користувачем, застосовується програма криптографування, перетворення текстового матеріалу у зашифрований. Особливого сенсу це набуває при електронному обміні інформаційними даними. Технологічно виглядає так: існує два електронні ключі – один з них має простий, а інший секретний код (ключова пара). Особа, яка передає мережею зв'язку електронний документ, кодує його за допомогою спеціальної програми — простого ключа і відправляє за вказаною адресою. Інший адресат, отримувач цих даних, може розшифрувати надіслану машинну інформацію при застосуванні другого (секретного) ключа, код якого йому відомий завчасно. Тобто для того, хто перехопив повідомлення, зашифровані дані залишаються таємницею. Спосіб криптографії вважається найбільш потужним засобом конфіденційності комп'ютерної інформації, як у самому комп'ютері, так і при передачі на інші магнітні носії. Існує велика кількість програмних забезпечень, які дозволяють шифрувати машинну інформацію, враховуючи різні умови аналізу шифротексту при спробах його розкодування. Деякі програми за умов стороннього втручання спрацьовують за інстинктом самозбереження. Зокрема, програма DISKREET з пакету NORTON Utilities окрім шифрування магнітних носіїв інформації виконує функцію блокування клавіатури, файлів – дисків вінчестера та відключення монітора. Здійснення подальшої роботи на комп'ютері відбувається через введення відповідного пароля [1, с. 45-47].

Дієвим є у криптографії застосування електронних ключів. Це програмне устаткування має обширну пам'ять і невеликі розміри мікросхеми. При запуску комп'ютера, програма перевіряє наявність свого ключа. Якщо такий ключ відшуковується, операційна система запускається і готова до роботи, якщо ж ні – видає повідомлення про помилку і допуск до роботи закривається.

Не менше важливим для дослідження є використання цифрового електронного підпису особи під конфіденційним документом та переадресування належному абоненту. Слід зазначити, що шифрування відбувається у зазначеному вище способі криптографії, в основі якого лежить ключова пара. Цифровий електронний підпис дає можливість не лише гарантувати аутентичність переданої машинної (комп'ютерної) інформації, а й перевірку достовірності характеристик авторства. Окрім того, ця система дозволяє перевірити увесь текст на наявність стороннього втручання та спробах його корегування. Вона здійснює хешфункцію (сумарне підрахування) видозміненого документа і перевірена сума повної або часткової фальсифікації тексту документа чи електронного підпису, буде відрізнятися від первинного її стану. Істинно підписаний та переадресований електронний документ повинен мати у собі окрім тексту, електронного підпису, – сертифікат користувача, в якому зазначені оригінальні дані абонента, що містять в собі дані імені та відкритий ключ розшифрування для перевірки підпису отримувачем або особою, що здійснила реєстрацію сертифіката.

Не є виключенням, є застосування криптографічного засобу і у цифрових мобільних телефонах, напади на які є вже «звичайним явищем». Нині існує достатня кількість спеціалізованих установ, що спеціалізуються на безпеці від перехоплень телефонних розмов власників зручного мобільного зв'язку. Першість у системі захисту інформаційних даних посідають провідні англійські компанії, які ввели і забезпечують захист розгалужену мережу цифрових мобільних телефонів. Кожний апарат має власний змішуючий код і всі розмови діють під окремим зашифруванням, перетворюючи речові сигнали на цифрові, щоразу змінні. Це так звані скремблери, які процюють у алгоритмі кодування і декодування у цифрових аналогових перетворювачах телефонних розмов.

Одним з важливіших інструментів у системі безпеки на сучасному етапі є ідентифікація, встановлення тотожності особи користувача за певними характеристиками. А саме:

за предметом, яким володіє користувач;

за паролем, особистим ідентифікаційним кодом, який вводиться в ЕОМ (комп'ютери) через клавіатуру;

за фізичними (антропометричними) характеристиками особи, які є неповторними по відношенню до неї;

за електронним цифровим підписом, що включає в себе криптографічну систему запису через ключову пару.

Особливу увагу слід зосередити на біометричних характеристиках ідентифікації та електронному цифровому підписі особи. Біометрія – спосіб ідентифікації особи за фізіологічними даними і порівнянні їх з базою схожих характеристик, що належать іншим людям. На відміну від традиційних методів ідентифікації біометрія має ряд переваг. Вона виключає наявність підтверджувальних документів при допуску роботи за операційною системою. У свою чергу:

а) не потребує жодних даних окрім самої особи;

б) фізіологічні дані людини не можуть бути загубленими, викраденими, підробленими, замішеними, скомпрометованими – завжди знаходяться при людині;

в) виключає проникнення сторонньої особи до операційної системи шляхом містифікації [2, с. 64 – 68].

Розробки з такими характеристиками є як у зарубіжній так і у вітчизняній практиці і їм прогнозують велике майбутнє, оскільки мова йде про ідентифікацію особи за сітчаткою очей людини. Науково підтверджено, що сітка кровоносних судин на сітчатці очей, як і папілярні типи візерунків пальців рук та ніг людини, є індивідуальними і не повторними, і видозмінити їх можливо лише тільки певним травмуванням або знищенням. В основі їх діяльності є пристрій, що містить вмонтовану фото-елементну камеру з електромеханічним сенсором, яка з близької відстані вимірює натуральне відображення сітчатки. Від особи,

яку ідентифікують вимагається секундна процедура — подивитися у спеціальний окуляр і прилад зафіксує структуру сітчатки ока та автоматично проведе тотожність з іншими, занесеними у базу даних комп'ютера даними і подасть відповідне звукове повідомлення допуску чи заборони. Людина може бути опізнаною в обсолютній точності зпоміж 1,5 тис. інших осіб і менше ніж до 5 секунд, а оперативна пам'ять таких розробок становить кілька тисяч осіб, що піддаються ідентифікації. Разом з тим зазначені наукові розробки можуть ідентифікувати особу за тембром голосу людини та папілярним типом візерунків пальців рук та ін., а також здійснювати:

— контроль доступу до мережевих систем;

контроль за кількістю відвідувачів за часом перебування;

контроль за сховищем цінних паперів, інших цінностей (зброї, грошових сум тощо);

контроль за перерахуванням грошей електронним шляхом та ін.

Підсумовуючи викладене, доходимо висновку, що захист інформації у сфері з використанням ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку перебуває у своєму потенційному розвитку і знаходить своє практичне застосування там, де використовуються комп'ютерні технології. До питань, пов'язаних з захистом інформаційного простору, а також безпечності від витоків комп'ютерної інформації під час її маршрутизації та інших несанкціонованих дій осіб з програмними забезпеченнями та їх електронними продуктами, долучаються вітчизняні та іноземні виробники з світовим визнанням. Вони створюють і пропонують споживачеві нові досконалі розробки програмних забезпечень направлених на захист витоків машинної інформації; програмно-апаратного модульного криптографічного захисту інформації; системи адміністрування й управління мережевими ресурсами; захисту електронної пошти; аутентифікації та контролю цілісності електронного документу; захисту корпоративних мереж з можливістю створення віртуальних корпоративних мереж; систем захищеного електронного секретного діловодства та ін. Такий широкий спектр запропонованого, вселяє віру в потенційних користувачів ЕОМ (комп'ютерних) систем, комп'ютерних мереж і мереж електрозв'язку, що їх машинна (електронна) інформація може бути надійно захищеною і цілісною, а значить не потрапить до рук тих, кому не адресувалася.

Література

1. *Авторский* коллектив под редакцией проф. П. С. Полевого. Правовая информатика и кибернетика. Учебник для высших учзаведений. — М. — «Юридическая литература», 1993. 264 с.

2. *Азаров Д.* Особливості механізму вчинення злочинів у сфері комп'ютерної інформації // Юридична Україна. 2004. № 7 (19). С. 64 68

3. *Баранов А. А., Брыжко В. М., Базанов Ю. К.* Защита персональных данных. ОАО «НПОТИ». К.,1998. 128 с.

4. *Біленчук П. Д., Романюк Б. В., Цимбалюк В. С.* Комп'ютерна злочинність. Навч. посіб. – К.: Атіка, 2002. – 240 с.

5. *Вехов В. Б.* Компьютерные преступления: Способы совершения и методика расследования / Под ред. Акад. Б.П. Смагоринского. – М.: Право и Закон, 1996. – 158 с.

6. *Колесник В.А.* Розслідування комп'ютерних злочинів. Наук.-метод. посіб. К.: Вид-во НА СБУ, 2003. 124 с.

7. *Романец Ю.В., Тимофеев А.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. М., 1999. 117 с.

А.И. Мотлях

Безопасность компьютерных информационных данных: нынешние реалии и перспективы.

В статье рассматриваются вопросы, связанные с обеспечением безопасности компьютерной информации в процессе ее обработки и передачи электронных данных, а также несанкционированных действий преступников с использованием ЭВМ (компьютеров), компьютерных систем и систем электросвязи.

In this article are examined questions which related to providing of safety of computer information in the process of its treatment and communication of electronic information and also the actions of criminals are unauthorized with the use of COMPUTER (computers) of the computers systems and systems of electrical connection.