ПРО ДЕЯКІ ЗАСОБИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ КОМП'ЮТЕРНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Мазниченко Наталя Іванівна
Національний юридичний університет імені Ярослава Мудрого
Україна

Життя сучасного суспільства неможливо уявити без використання сучасних інформаційних технологій. Активне впровадження сучасної комп'ютерної техніки та мережевих технологій в будь-яку сферу життя майже кожної людини призвело до того, що величезні обсяги різноманітної інформації в цифровій формі зберігаються в комп'ютерних системах та передаються з використанням комп'ютерних мереж. Серед всього обсягу інформаційних ресурсів є інформація, що має статус конфіденційної і потребує обмеження в доступі. Це може бути інформація, що містить державну таємницю, комерційну таємниці, особисті данні і таке інше. Природно, виникає потреба захистити таку інформацію від несанкціонованого доступу, крадіжки, знищення і інших злочинних дій. Концентрація інформації в цифровій формі в комп'ютерних системах примушує все більше приділяти увагу задачі її захисту. Питання безпеки і захисту інформації в комп'ютерних системах та мережах від несанкціонованого доступу є важливими та актуальними на сьогоднішній день. В останні роки проблеми, пов'язані із захистом інформації турбують як фахівців в галузі комп'ютерної безпеки, так і численних звичайних користувачів персональних комп'ютерів. Дослідження в цьому напрямку призвели до виникнення окремої галузі – інформаційної безпеки. Інформаційна безпека має декілька аспектів: правовий, програмно-технічний, організаційний, морально-етичний. Розглянемо та проаналізуємо сучасні методи та засоби програмного захисту комп'ютерної інформації, яка вважається конфіденційною.

В деяких організаціях, підприємствах, установах, компаніях існують спеціальні структурні підрозділи інформаційної безпеки і саме вони повинні розробляти політику безпеки, яка повинна бути адекватною потенційним загрозам. Спеціалісти в області безпеки інформації відповідають за розробку, реалізацію та експлуатацію систем забезпечення інформаційної безпеки, спрямованих на підтримку цілісності, доступності та конфіденційності накопиченої комп'ютерної інформації. Але звичайні користувачі також можуть мати інформацію, яку вони вважають

конфіденційною і не бажають ділитися нею зі всіма. Нажаль, більшість користувачів не усвідомлює, що постійно ризикує безпекою власної інформації і особистими таємницями, і лише деякі з них хоча б якимось чином захищають дані, які вважають конфіденційними. Для того, щоб захистити особисту інформацію від несанкціонованого доступу користувачам потрібно добре орієнтуватись в сучасних методах та способах захисту комп'ютерної інформації. Спробуємо розглянути особливості та специфіку кожного з захисних механізмів та систематизувати їх.

Сьогодні в області безпеки інформаційних комп'ютерних систем застосовуються різноманітні технології захисту. Розглянемо ті, що можуть бути використані звичайними користувачами для захисту конфіденційної інформації, дослідимо переваги та недоліки кожної з них.

По-перше, проаналізуємо можливості захисту конфіденційної інформації в цифровій формі за рахунок обмеження доступу до неї на основі систем ідентифікації користувачів. В таких системах доступ користувачів до різних класів інформації визначається ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача. Сьогодні існують наступні найпоширеніші підходи до ідентифікації користувачів [1, с. 216]:

1). Парольна ідентифікація. В даному випадку кожен зареєстрований користувач комп'ютерної системи отримує набір персональних реквізитів (в даному випадку використаються пари логин-пароль). Ну а оскільки вони унікальні для кожного користувача, то на їх підставі система й робить висновок про особу та ідентифікує її. Головна перевага парольної ідентифікації − це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною. При правильному використанні паролі можуть забезпечити прийнятний для багатьох користувачів рівень безпеки.

Недоліки даного підходу добре відомі, пароль може бути скомпрометованим багатьма способами. Саме слабкий рівень парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу. Але на сьогоднішній день символьний пароль є найпоширенішим способом ідентифікації користувачів.

2). Апаратна (електронна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера. Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті електронних пристроїв може зберігатися інформація, підібрати які досить складно. Крім того, у них реалізовано чимало різних захисних механізмів. Найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є можливість

крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Ще один мінус розглянутої технології – ціна, яку на сьогоднішній день неможливо вважати загальнодоступною, адже для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними електронними ключами. Крім того, згодом деякі типи ключів можуть зношуватися, крім того, вони можуть бути загублені й т.д.

3). Біометрична ідентифікація. Біометрія – це ідентифікація людини по унікальним, властивим тільки йому біологічним ознакам. Сьогодні експлуатується вже більше десятка різних біометричних ознак: відбиток пальця, сітківка ока, райдужна оболонка ока, зображення обличчя, голос і т.д. Головною перевагою біометричних технологій є найвища надійність, тому що вважається, що не буває різних людей з однаковими біометричними характеристиками. Основним недоліком біометричної ідентифікації є вартість устаткування, адже для кожного комп'ютера необхідно придбати окремий сканер. Звичайно, останнім часом ціни на біометричні пристрої постійно знижуються. Крім того, все більше з'являється мобільних пристроїв з вбудованими можливостями ідентифікації користувача по відбитку пальця або по зображенню обличчя, але важко назвати таку технологію поширеною.

Слід відзначити, що останнім часом для підвищення рівня захищеності інформаційних ресурсів комп'ютерних систем використовують комплексні або багатофакторні системи ідентифікації [2]. В таких системах для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів. Причому комбінуватися ці параметри можуть у довільному порядку. Наприклад, в біоелектронних системах для захисту комп'ютерної інформації від несанкціонованого доступу застосовується комбінація з двох систем − біометричної (наприклад, відбиток пальця або інша ознака) і електронної на базі смарт-карт або USB-ключів. Також останнім часом все більшого поширення набувають системи, що поєднують парольну ідентифікацію з визначенням користувача по клавіатурному почерку (особливостями введення паролю). Втім, сьогодні в переважній більшості випадків використається тільки одна пара: парольний захист і токен.

Другим поширеним способом захисту конфіденційної інформації є шифрування (криптографія). Під криптографічним захистом інформації розуміється таке перетворення вихідної інформації, в результаті якого вона стає недоступною для ознайомлення та використання особами, що не мають на це повноважень. Криптографічні методи захисту інформації застосовуються як для захисту інформації, що обробляється та зберігається на окремому комп'ютері, так і для захисту інформації, що передається по мережах.

Сьогодні розроблена велика кількість різних методів шифрування, створені теоретичні та практичні основи їх застосування.

Процес шифрування полягає в перетворенні вихідної інформації, в

результаті якої зашифрована інформація являє собою хаотичний набір незрозумілих символів. Для шифрування інформації використовують алгоритм перетворення і ключ. Шифрування дає можливість перетворити інформацію таким чином, що її читання можливе тільки при наявності ключа.

За особливостями алгоритму шифрування буває симетричним та асиметричним. В симетричних криптосистемах однин те й самий ключ використовується для шифрування та дешифрації (повернення інформації в початковий стан). Симетричне шифрування доцільно використовувати для збереження інформації в захищеному виді на локальному комп'ютері (немає потреби передавати ключ іншому користувачеві). В асиметричних криптосистемах (системах з відкритим ключем) використовується два ключі: відкритий ключ – для шифрування та відповідний йому секретний – для розшифрування. Асиметричне шифрування доцільно використовувати при необхідності передачі конфіденційної інформації по комп'ютерним мережам, оскільки передача партнерові за перепискою по мережі відкритого ключа не представляє небезпеки (вважається, що визначити закритий ключ по відкритому неможливо). В свою чергу секретний ключ належить тільки його власнику і тримається в таємниці. На сьогоднішній день асиметричне шифрування вважається найбільш надійним способом захисту комп'ютерної інформації від несанкціонованого доступу.

Розглянемо ще одну технологією, що застосовується в області захисту конфіденційної інформації − цифрову стеганографію, що активно розвивається останніми роками. Стеганографія (з грецької – тайнопис) – наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. Цифрова стеганографія – напрямок класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, що викликає деякі зміни цих об'єктів [3]. Але, як правило, такі об'єкти є мультимедіа-об'єктами (зображення, аудіо, відео-файли, 3-D об'єкти) і внесення змін, що знаходяться нижче порога чутливості середньо статистичної людини, не призводить до помітних змін цих об'єктів. Цифрова стеганографія має декілька напрямків застосування, одним з яких є вбудовування інформації з метою її прихованої передачі. Захист конфіденційної інформації здійснюється за рахунок приховування секретної інформації в цифровій формі всередині іншої інформації в цифровій формі від необізнаного користувача. Основна мета – непомітність даного впровадження секретної інформації в інший файл (контейнер), яка реалізується за рахунок надмірності, що є в цифрових сигналах (графіка, звук, відео, текст). Тобто, після впровадження секрету в файл-контейнер (отримаємо стегоконтейнер) він не буде пригортати особливої уваги і необізнаний користувач звичайними органами почуттів ніяких змін не помітить. Таким чином можна передавати по мережах конфіденційну інформацію, яка буде прихована від сторонніх. Користувач, для якого ця інформація призначалась, зможе її витягнути. На сьогоднішній день на ринку програмного забезпечення існує достатня кількість програм, що використовують дану технологію і звичайним користувачам є з чого

вибирати.

Деякі автори досліджень в області інформаційної безпеки вважають способом захисту комп'ютерної інформації використання ЕЦП (електронного цифрового підпису). Не можу погодитись з такою думкою. У питанні захисту конфіденційної інформації від несанкціонованого доступу звичайне використання ЕЦП навряд дозволить досягти поставленої мети. Основні функції та призначення ЕЦП – ідентифікація та аутентифікація електронних документів. Тобто, Підписаний ЕЦП документ дозволяє встановити автора (підписувача) даного документа та визначити, чи були внесені зміни в документ після його підписання (наприклад, під час передачі по мережі). Але безпосередньо захисної функції (без використання додаткових механізмів захисту) від стороннього несанкціонованого втручання у ЕЦП немає. Але якщо підписаний ЕЦП документ зашифрувати, то таким чином можна його захистити від несанкціонованого доступу з додатковими перевагами, які надає ЕЦП.

Наприкінці хотілося б наголосити, що потрібно чітко уявляти собі, що ніякі апаратні, програмні і будь-які інші рішення не зможуть гарантувати абсолютну надійність і безпеку даних в інформаційних системах. Так само слід пам'ятати, що велика концентрація захисних засобів в інформаційній системі може привести не лише до того, що система виявиться дуже дорогою, але і до того, що можна отримати її перевантаження і зниження продуктивності. Тому головне при визначенні заходів захисту інформації − це кваліфіковано визначити межі розумної безпеки і витрат на засоби захисту з одного боку і підтримки системи в працездатному стані і прийнятного ризику з іншого.

На основі аналізу розглянутих технологій можна порадити користувачам спочатку оцінити важливість та рівень секретності інформації, що потребує захисту та обмеження в доступі і тільки після цього обрати відповідні механізми захисту, які будуть адекватно відповідати можливим потенційним загрозам. Проте практика показує, що для надійного захисту конфіденційної інформації тільки комплекс заходів здатний допомогти в досягненні поставленої мети.

Список використаних джерел:

1. Кошева Н.А. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів [Текст] / Н.А. Кошева, Н.І. Мазниченко // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с. – С. 215-223
2. Шрамко В.Н. Комбинированные системы идентификации и аутентификации [Электронный ресурс] // PCWeek/RE. − 2004. − №45. − Режим доступа: http://www.bre.ru/security/25022.html
3. Каас А. Цифровая стеганография [Электронный ресурс] // TPL-IT. – 2010. − Режим доступа: http://tpl-it.wikispaces.com/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F+%D1%81%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«ЄВРОПЕЙСЬКА НАУКОВА ПЛАТФОРМА»

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

АКТУАЛЬНІ ПИТАННЯ СЬОГОДЕННЯ

20 березня 2018 рік | м. Вінниця

ТОМ 9

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ΛΌΓΟΣ

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«ЄВРОПЕЙСЬКА НАУКОВА ПЛАТФОРМА»
ОО «ЕВРОПЕЙСКАЯ НАУЧНАЯ ПЛАТФОРМА» ◊ NGO «EUROPEAN SCIENTIFIC PLATFORM»

ЗБІРНИК НАУКОВИХ ПРАЦЬ «ΛΌГОΣ»

МАТЕРІАЛИ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«АКТУАЛЬНІ ПИТАННЯ СЬОГОДЕННЯ»

20 БЕРЕЗНЯ 2018 РІК

ТОМ 9

м. Вінниця

УДК 001(08)
ББК 72.4(4УКР)я 431
Н 34

Н 34 **Актуальні питання сьогодення** [текст]: матеріали Міжнародної науково-практичної конференції 20 березня 2018 року у м. Вінниця: зб. наук. праць «ΛΌГОΣ» / відп. за випуск Голденблат М.А. // ГО «Європейська наукова платформа». – Обухів: Друкарня «Друкарик» (ФОП Гуляєва В.М.), 2018. – Т.9. – с.124.

Викладено тези доповідей та статті учасників міжнародної науково-практичної конференції «Актуальні питання сьогодення», яка відбулася у місті Вінниця, 20 березня 2018 року.

Збірник присвячено для студентів, аспірантів, докторантів, здобувачів, молодих фахівців, викладачів, науковців та інших зацікавлених осіб, а також для широкого кола читачів.

Бібліографічний опис матеріалів конференції представлено у Науковій електронній бібліотеці «Elibrary.ru».

Зібрник включено до міжнародних наукометричних баз «РИНЦ» та «Google Академія».

УДК 001 (08)
ББК 72.4(4УКР)я 431