Коцюк Ю. А.

РОЛЬ ЛЮДСЬКОГО ЧИННИКА У ПИТАННЯХ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті розглядається роль людського чинника у питаннях захисту інформаційних систем, зокрема досліджується ставлення людей до паролів.

Ключові слова: *пароль, людський чинник, інформаційні системи, інформаційна безпека, особливості запам’ятовування.*

В статье рассматривается актуальный вопрос человеческого фактора в вопросах защиты информационных систем, в частности исследуется отношение людей к паролям.

Ключевые слова: *пароль, человеческий фактор, информационные системы, информационная безопасность, особенности запоминания.*

The article considers the current issue of the human factor in the protection of informational systems; in particular, we investigate people’s attitude to passwords.

Keywords: *password, the human factor, informational systems, informational security, memory peculiarities.*

Сучасний етап розвитку суспільства неможливо розглядати відокремлено від технічного прогресу і зокрема від інформаційних систем. Інформаційні системи використовуються практично в усіх сферах життя суспільства. Вони надають зручне середовище для роботи, навчання, розміщення та обміну інформації; вони дозволяють спілкуватися, забезпечують зручні сервіси для банківської, комерційної діяльності, зрештою, займають великий сектор ігрової індустрії. Спробувавши хоча б раз сервіси інформаційних систем та оцінивши їх переваги, відмовитися від них вже практично неможливо. Будь-яка інформаційна системи працює з інформацією, у тому числі й з конфіденційною, тому однією із серйозних вимог, що ставляться до таких систем, є реалізація інформаційної безпеки. Питання інформаційного захисту неодноразово висвітлювалися як у наукових працях, так і в періодичних виданнях вітчизняних та зарубіжних

вчених (Б. Ю. Анін, М. І. Анохін, В. Ю. Артемов, С. У. Баричев, В. О. Бондаренко, В. О. Голубєв, В. В. Гончаров, М. А. Іванов, В. Г. Крисько О. В. Литвиненко, В. Н. Петров, А. А. Петров, М. М. Присяжнюк, В. С. Пущін, В. С. Сідак, А. Г. Серго, В. В. Ященко). Слід відзначити, що у більшості публікацій розглядаються загальні питання інформаційної безпеки держави, суспільства, організації, особистості, причому, перевага надається опису технічних засобів чи інформаційних технологій, покликаних реалізувати інформаційний захист. Проте використання інформаційних технологій, з одного боку, справляє значний вплив на свідомість людей, а з іншого, надає колосальні можливості тим, хто вміє їх використовувати. Така ситуація призводить до зростання ролі людського чинника у питаннях інформаційного захисту.

Метою статті є дослідження ставлення користувачів інформаційних систем до реалізації їх захисту, зокрема наголос робиться на використанні паролів.

Завдяки процесам глобалізації більшість інформаційних систем мають територіальний розподіл. Проте, не зважаючи на це, усі вони переважно орієнтуються на конкретного користувача. Так, враховуються регіональні стандарти: мова, грошові одиниці, локальний час тощо. Ці параметри можуть бути згенеровані лише завдяки місцю розташування користувача. Інші ж преференції користувачів вимагають ідентифікації. Ідентифікація користувачів в інформаційних системах можлива з допомогою імені користувача (логіну), яке вводиться у відповідне поле, і подальшого вводу паролю з метою автентифікації. Якщо автентифікація проходить успішно, то користувач отримує статус авторизованого користувача. Механізм авторизації дозволяє організувати керування рівнями та засобами доступу до різних об'єктів та ресурсів; надавати певні повноваження користувачеві на виконання певних дій; визначати міру приватності даних тощо. Існують й інші способи ідентифікації, наприклад за IP-адресою, проте такі способи дозволяють ідентифікувати радше робоче місце/обладнання, а не користувача. Тому схема логін-пароль поки що лишається єдиним ефективним засобом ідентифікації.

Проблему захищеності інформації в інформаційних системах сьогодні вирішують шляхом використання криптографічних засобів. Використання криптографії дозволяє реалізувати такі основні можливості:

– захист інформації шляхом її шифрування з допомогою ключа;

– автентичність інформації – можливо за рахунок електронного цифрового підпису;

– автентичність підписувача – можливо за рахунок електронного цифрового підпису.

Шифрування інформації здійснюється з метою запобігання її викрадення. Навіть якщо зловмисник певним чином отримає доступ до зашифрованої інформації, він не зможе її прочитати без спеціального ключа.

Автентичність інформації потрібна для того, щоб переконатися, що з моменту підписування вона не змінювалася. Так, підписаний з використанням цифрового підпису наказ чи звіт можна вважати справжнім.

Автентичність підписувача дозволяє підтвердити авторство інформації. Важливо це з кількох міркувань:

Якщо документ підписаний авторитетним автором, то й довіра до змісту написаного буде висока.

Інший приклад – перевірка справжності веб-сайтів. Справжність веб-сайтів важлива при роботі з веб-сайтами банків чи платіжних систем. Якщо користувач відвідує веб-сайт без електронного цифрового підпису, то велика імовірність не помітити підробку.

Криптографічні системи мають високу стійкість до зламу та характеризуються високою надійністю, проте вони не враховують людський чинник. Справа в тому, що доступ до ключів, з допомогою яких здійснюються операції розшифровування та накладання електронного цифрового підпису, здійснюється з допомого паролю. У більшості випадків користувач має можливість самостійно створювати пароль з врахуванням деяких обмежень системи.

Як показує статистика, більшість користувачів відчувають певний дискомфорт при створенні паролів. З одного боку, занадто простий пароль використовувати небезпечно, з іншого – складний пароль важко запам’ятати. Користувачі, які мають слабке уявлення про функціонування систем захисту інформації, допускаються серйозних помилок при створенні паролів. Список типових помилок такий:

Надто простий пароль:

– використання дати народження як пароля;

– використання прізвища, імені, по батькові або ж їх комбінацій як пароля;

– використання типових паролів, таких як “qwerty”, “123456”, “password”, “******” (шість зірочок) тощо;

– використання назви обладнання на робочому столі як паролів (див. рис. 1.), відповідно як пароль використано назву ноутбука – “ProBook 4530s”.

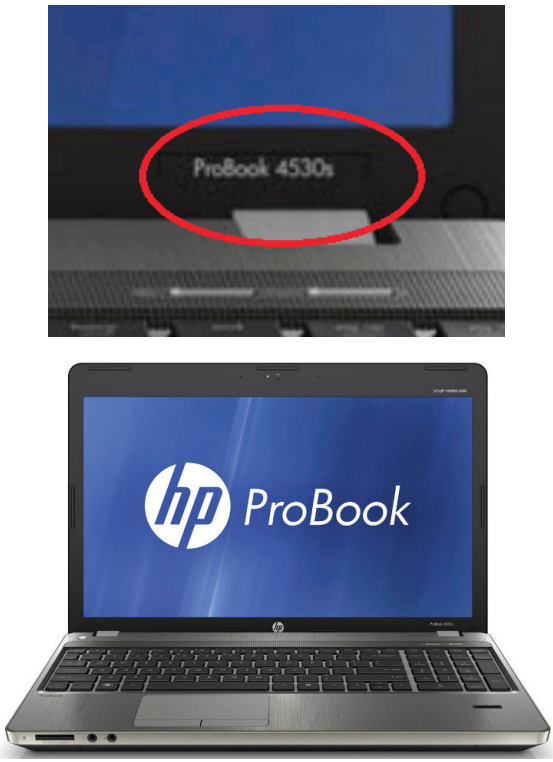

Рис. 1. Приклад використання як пароля назви ноутбука

Більшість користувачів обирає варіант: один однаковий пароль на усі ресурси. І знову ж таки пріоритетом у виборі такого рішення стає зручність, або ж уявлення про комфортність. Звичайно ж, один пароль запам'ятати набагато легше, ніж тримати у пам'яті велику кількість логінів та паролів. Проте уявлення про комфорт різко змінюється, якщо ознайомити користувача з основами інформаційної безпеки. Якщо зловмисник отримує доступ хоча б до одного ресурсу, він автоматично отримує доступ і до решти. У більшості випадків інформаційна безпека, як складова психологічного комфорту, набуває першочергового значення у користувачів, у яких хоча б раз поцупили пароль. Тим же, хто надає перевагу одному простому паролю для усіх інформаційних систем, керуючись у першу чергу зручністю, мож-

на порекомендувати хоча б розділити усі свої ресурси на дві чи три групи з точки зору важливості. Перша група – серйозні інформаційні системи, які працюють з конфіденційною чи фінансовою інформацією. Сюди можна зарахувати такі системи, як онлайн-банкінг, платіжні системи, корпоративні інформаційні системи. Друга група – інформаційні системи, пов’язані з обміном інформації чи діловим листуванням. В основному це системи обробки електронної пошти, системи обміну миттєвими повідомленнями, системи відео- чи аудіочатів. Третя група – інформаційні системи форумів, блогів, розважальних послуг. Відповідно, при такому групуванні достатньо запам’ятати всього три паролі, перший з яких повинен бути доволі складним, другий – середньої складності і третій може бути доволі простим.

Зберігання паролів:

Практично усі браузери (програми для здійснення навігації в Інтернет), дозволяють зберегти логін і пароль входу до інформаційної системи. Причому є можливість для різних систем запам’ятати навіть різні паролі, а деякі браузери навіть вміють використовувати один “майстер-пароль”, який використовується для шифрування решти паролів. Тому багато користувачів використовують цю можливість. Слід звернути увагу у цьому випадку на декілька моментів. Перше – не варто використовувати цю можливість у публічних місцях, інакше будь-який користувач, який працюватиме на тому ж робочому місці, зможе скористатися чужим логіном і паролем. Друге – навіть використання такої можливості на домашньому, персональному комп’ютері небезпечне, оскільки при роботі в мережі Інтернет у зловмисника існує можливість отримати доступ до місця збереження паролів.

Збереження логіна й пароля у текстовому файлі – можливість, яка має такі ж недоліки, як і в попередньому випадку. Отримавши доступ до файлу, зловмисник отримує доступ до усіх логінів і паролів. Якщо ж текстовий файл зберігається на змінному носієві – існує можливість пошкодження носія, а з ним і самого файлу.

Збереження логіна й пароля у мобільному телефоні – можливість, яку використовує значна кількість користувачів. Основна небезпека – викрадення телефону.

Збереження логіна й пароля на паперових носіях. Знову ж таки, основна небезпека – викрадення такого паперового носія. Так, наприклад, якщо зберігати у гаманці і платіжну картку, і пін-код до неї, написаний на папірці, то при викраденні гаманця зловмисник отримає подарунок у вигляді “картка+пін-код”. Жіноча ж сумочка, де зберігається і гаманець, і мобільний телефон, для зловмисника буде

справжнім скарбом. Якщо ж паперовий носій, на якому записано пароль, зберігається в офісі, то найчастіше його "ховають" у таких місцях: під клавіатурою, під телефоном, у якій-небудь верхній шухляді, під кришкою стола. Найгірший варіант – пароль написаний на стікері й приліплений до кутка монітора.

Передача у користування свого пароля друзям, рідним, знайомим, співробітникаи. Це найбільш груба помилка у користуванні інформаційними системами. Особливо неприємна ситуація, коли власник пароля передавав його двом чи навіть трьом різним особам. Крім зростання ймовірності дискредитації пароля, власник може зіткнутися з моральною проблемою довіри до людей, які знають його пароль.

Поряд з помилками, які допускають користувачі при створенні та використанні паролів, слід також навести основні шляхи, якими зловмисники здобувають чужі паролі. Знання цієї інформації дозволить підвищити рівень психологічного комфорту при роботі з інформаційними системами, змінивши уявлення у користувачів про комфорт як такий через зміщення пріоритету від зручності у бік безпечності.

Отож, яким чином "крадуть" паролі:

Використання методів соціального інжинірингу чи соціальних технік [3; 6]. Потрібний пароль дуже часто можна просто запитати, і в багатьох випадках його повідомляють. Зловмисник може при цьому представлятися обслуговуючим персоналом, вищим за рангом службовцем, перевіряючим, новим працівником поки що без свого логіна й пароля. Дуже часто для цього використовується телефон. Цей спосіб є найпростішим, і саме з найпростіших способів зловмисники починають. Так у ході недавнього дослідження фірма PentaSafe Security Technologies виявила, що четверо з п'яти працівників готові повідомити свої паролі комусь із товаришів по службі, якщо ті про це попросять. У ході іншого дослідження тієї ж компанії майже дві третини службовців, опитаних на вокзалі Вікторія в Лондоні, виклали свій пароль за дешеву авторучку [8].

Вгадування пароля. Метод, який базується на підборі слабких часто вживаних паролів. Як не дивно за ефективністю він займає друге місце. Часто, щоб "вгадати" такий пароль, потрібно мати загальне уявлення про людину, про її рідню тощо. І такою інформацією охоче діляться користувачі соціальних мереж.

Спроба підібрати пароль шляхом звичайного перебору всіх можливих варіантів – так звана атака Brute force. Такий метод можливий при використанні потенціалу комп'ютерної техніки. При оцінці швидкості його роботи виходять з припущення, що за одну секунду

комп’ютер може перевірити 100 паролів. Обмеження у 100 паролів накладається не можливостями комп’ютера, а власне самою системою [1].

Спроба підібрати пароль за поширеними словами – простіший різновид Brute force, який займає набагато менше часу.

Атака за словником – передбачає перебір можливих слів словника.

Крадіжка пароля за допомогою комп’ютерних вірусів чи інших зловмисних програм – передбачає враження комп’ютера вірусом, який “цупить” пароль і через мережу передає його власнику віруса.

До паролів ставляться доволі жорсткі вимоги. Так, довжина пароля не повинна бути коротша 8-ми символів, слід використовувати і символи верхнього, і символи нижнього регістру, цифри, бажане використання спеціальних символів. Крім того, не рекомендується використовувати як пароля власне ім’я, прізвище, зменшене ім’я тощо. Ідеальний пароль – пароль, що складається із сукупності випадкових символів. Зрозуміло, що запам’ятати такий пароль доволі складно. А якщо додати вимогу щодо періодичної зміни паролів, то ситуація ускладниться ще більше.

І все ж є декілька способів створення “сильних” паролів, які легко запам’ятати:

Використання перших чи останніх букв непопулярного віршика чи вислову. Спосіб цей доволі поширений [5; 8; 9].

Так для прикладу розглянемо дитячий віршик “Хлопчик Помагай”.

Через ***п***оле ***ч***ерез ***г***ай

Ходить ***Х***лопчик ***П***омагай

Якщо “зібрати” до купи перші літери кожного слова, отримаємо щось на кшталт “ЧпчгХХП”. Додамо декілька цифр, наприклад 4 і 3 (можна проасоціювати це собі так: 4 великих символи і 3 маленьких) і отримаємо “4ЧпчгХХП3”. Оскільки більшість систем вимагають пароль латинськими символами, перетворюємо нашу фразу на латинку одним з кількох способів:

– транслітерація – “4CHpchhkhKHP3”, або ж так: “44n4sxXKN3”, або ж так, як підказує власна логіка;

– використання латинської клавіатури для кириличних символів. Кожен кириличний символ на клавіатурі має свій латинський відповідник, тому, якщо набирати пароль кирилицею з латинською (англійською) розкладкою клавіатури, отримає такий пароль: “4Xgxu[{G3” (див. рис. 2).

Зрозуміло, що “кодова фраза” може бути використана будь-якою мовою. Це може навіть бути особистий переклад якось важливої фрази з іноземної.

Рис. 2. Відповідність на клавіатурі символам кирилиці символів латинки

Такий пароль “запам’ятовують” пальці. І навіть спроба написати власний пароль авторучкою на папері може виявитися невдалою.

Генерація складного паролю спеціальними генераторами (у мережі Інтернет їх можна знайти доволі багато) і запам’ятовування його. Звичайно можна спробувати використати якийсь асоціативний метод, але це не завжди спрацьовує. Простіше механічно “завчити” пароль, увівши його на клавіатурі разів 20, а то й більше (залежить від індивідуальних особливостей). Знову ж таки, “пам’ятатимуть” пароль пальці.

Використання як паролі фраз, що являють собою синоніми, антоніми в різних комбінаціях із розділовими знаками, повтори, перебільшення (“сфера, галузь діяльності”, “холодний жар”, “важка легкість, “Цукровий цукор на клавіатурі”, “найкривіша пряма лінія” тощо). Якщо у системі існує заборона на використання пробілів, замість них можна використовувати символ “_”.

Останній метод створення паролів доволі дієвий, оскільки пароль має високу надійність і його легко запам’ятати (див. рис. 3).

Type	Password	Method	Time	Security level
2 common word password	alpine fun	Common word	2 months	Low risk
3 common word password	this is fun	Common word	2,537 years	Secure forever

Рис. 3. Надійність пароля, що складається з 2 та 3 слів до атаки підбором широковживаних слів

Вище вказана статистика наведена з врахуванням можливості зловмисника підбирати 100 паролів за секунду [1]. Таким чином, щоб здолати пароль з двох звичайних слів методом підбору за звичайними словами, потрібно 2 місяці, у той час як пароль з трьох слів потребуватиме 2 537 років[1]. До слова, інші способи атаки в цьому випадку будуть менш ефективні:

[1] Статистика наведена для англійських поширених слів, проте схожа ситуація буде і при використанні іншомовних слів, оскільки атака здійснюється з допомогою так званого словника хакера, а його можна наповнювати довільним чином.

– атака типу brute-force – 1 163 859 років[1];

– атака за словником – 39 637 240 років[2][1].

Над усуненням людського фактора у безпеці інформаційних систем працюють також і самі розробники цих систем. Так основними принципами, які використовуються при розробці будь-яких інформаційних систем, є максимальна простота та інтуїтивність інтерфейсу, з одного боку, а також відсутність в інтерфейсі можливості нашкодити системі з боку користувача.

Що ж до паролів, то більшість систем відразу перевіряють пароль на надійність і вказують користувачу ступінь його надійності. Разом з тим у більшості систем існує заборона на надто “слабкий” пароль.

За таких обставин розробники змушені “турбуватися” і про відновлення забутого пароля. Існує декілька способів відновити втрачений пароль:

– відновлення з допомогою слова-підказки (доволі неефективний спосіб, оскільки користувачі зазвичай забувають і пароль, і слово-підказку);

– відновлення з допомогою адреси електронної скриньки (у цьому випадку посилання на відновлення паролю відсилається на електронну скриньку користувача, при цьому користувач повинен використовувати надійний пароль до самої електронної скриньки, інакше цим способом може скористатися і зловмисник);

– відновлення з допомогою мобільного телефону (код підтвердження відновлення пароля відсилається на мобільний телефон; недолік – телефон можуть поцупити).

Крім звичайних паролів деякі системи використовують подвійну автентифікацію:

– використання поряд із введенням пароля надсилання коду підтвердження на мобільний телефон (платіжні системи);

– використання поряд із введенням постійного пароля списку одноразових паролів (банківські системи; список одноразових паролів може роздрукувати власник платіжної картки на терміналі банкомату);

– використання як альтернативи звичайному паролю цифровий пароль, що зберігається на флеш-носії (інформаційна система Windows та інші);

використання як альтернативи звичайному паролю або разом із

[1] Статистичні дані наведені з врахуванням того, що пароль може містити цифри, латинські символи верхнього чи нижнього регістру а також спецсимволи.

[2] Дані справедливі для англомовного словника.

ним відбитків пальців (інформаційна система Windows та інші, за умови, що є система зчитування відбитків пальців).

Підсумовуючи усе вище сказане, можна зробити висновок, що одне з найважливіших місць у безпеці інформаційних систем посідає людський фактор. І нехтування його може становити загрозу не лише окремій особистості, а й цілій організації. Тому слід проводити регулярну роботу з користувачами інформаційних систем як у навчальних закладах, так і в організаціях. Завданням цієї роботи повинно стати набуття комплексу знань в царині інформаційної безпеки. Причому такий комплекс знань дозволить не лише набути навичок безпечної роботи з інформаційними системами та паролями, а й дозволить усвідомити необхідність стійких паролів шляхом формування інформаційної складової психологічного комфорту [7].

Перспективами подальших досліджень у цьому напрямі може стати розробка навчальних курсів, навчальних презентацій та роздаткових матеріалів з питань інформаційної безпеки для користувачів інформаційних систем, а також дослідження зміщення пріоритету в питаннях використання паролів від зручності до безпеки.

Література:

1. Baekdal T. The Usability of Passwords [Електронний ресурс] / Thomas Baekdal // Baekdal – The New Media Magazine. – (AUGUST 11, 2007). – Умови доступності : http://www. baekdal. com/insights/password-security-usability.

2. GolDenOne Простой и надежный пароль – коллективное творчество [Електронний ресурс] / GolDenOne // Хабрахабр. – (1 мая 2011, 19:49). – Умови доступності : http://habrahabr. ru/post/118499/.

3. Granger S. Основы социотехники (искусства обмана), часть 1. Тактика хакеров [Електронний ресурс] / Sarah Granger // Центр исследования проблем компьютерной преступности / Crime-Research. org. – [2004?]. – Умови доступності : http://www. crime-research. ru/news/02. 11. 2004/1584/.

4. Анин Б. Ю. Защита компьютерной информации : практическое пособие / Б. Ю. Анин. – СПб. : BHV-Санкт-Петербург, 2000. – 368 с : ил.

5. Гаранькін О. Як запам'ятати пароль [Електронний ресурс] / Олександр Гаранькін // Як просто. – (23. 01. 2012 03:35). – Умови доступності : http://yak-prosto. com/yak-zapam-yatati-parol/.

6. Котадиа М. Социальный инжиниринг – главная угроза для безопасности [Електронний ресурс] / Мюнир Котадиа // Центр исследования компьютерной преступности / Computer Crime Research Center. – (02. 11. 2004). – Умови доступності : http://www. crime-research. ru/news/02. 11. 2004/1584/.

7. Коцюк Ю. А. Криптографічні методи захисту інформації та психологічний комфорт користувачів інформаційних систем [Електронний ресурс] / Ю. А. Коцюк // Інформаційні технології і засоби навчання. – Грудень 2007. – № 3. – Умови доступності : http://www. nbuv. gov. ua/e-journals/ITZN/em3/emg. html.

8. Найпоширеніші паролі [Електронний ресурс] // Комп’ютерні записи. – (14 січеня, 2009 р. 23:21). – Умови доступності : http://compik. ks. ua/najposhyrenishi-paroli/.

9. Янчук О. Створення пароля, який легко запам’ятати – практичні поради [Електронний ресурс] / Олексій Янчук // ISearch. – [2010-10-31]. – Умови доступності : http://isearch. kiev. ua/en/-searchpractice-en/-internetsecurity-ru/1234-samples-vhdl-create-a-password-that-is-easy-to-remember-practical-advice.