діяльності людини, полягає у виявленні їх властивостей з метою прогнозування поведінки об'єкта системи та вибору оптимального керування ними. Диференціальні рівняння широко використовуються на практиці, зокрема для опису перехідних процесів, коливань, теплопровідності, деформації балок і пластин, поширення електричного струму у провіднику тощо.

Список використаних джерел

1. Матохнюк Л. О., Блінніков Г. П. Методика розв'язування прикладних задач за допомогою диференціальних рівнянь. 2011, С. 388–399.
2. Найко Д. А., Новицька Л. І. Завдання з математики для студентів агрономічного факультету: збірник завдань з математики для проведення практичних, лабораторних занять, організації самостійної роботи зі студентами агрономічного факультету. Вінниця: Видавничий центр ВДАУ, 2006, 71 с.
3. Кремень В. Освіта в XXI столітті має стати пріоритетом у будь-якому суспільстві. *Математика в школі*. 2002. С. 2–4.

Андрій Рожанський,
Ігор Дружинін,
Леон Рокочук,
Роман Діденко

БЕЗПЕКА ПОЧИНАЄТЬСЯ З ПАРОЛІВ

В еру стрімкого розвитку та масового розповсюдження інформаційно-комунікаційних технологій, без яких сучасне суспільство не може обійтися, досить гостро постає питання безпеки. Кожен користувач, використовує як мінімум два пристрої: комп'ютер/ноутбук і смартфон, але не завжди задумується про необхідність встановлення належного захисту на свої гаджети. Саме тому, слід приділяти даному аспекту значної уваги [1]. Наразі, навіть найкращі методи безпеки не можуть гарантувати 100 % захист даних користувачів, але відмова від їх використання взагалі знижує рівень безпеки до нуля. Шкідливі програмні засоби постійно модифікуються їх розробниками для того, щоб обійти всі можливі засоби захисту, але і розробники засобів для забезпечення безпеки постійно оновлюють сигнатури своїх продуктів, що дозволяє знешкоджувати більшість загроз. Звісно, якщо сам користувач не дозволить виконання підозрілої програми або відкриє заражений файл та проігнорує застереження.

Авторизований доступ до своїх гаджетів, програм, онлайн сервісів тощо користувачі отримують за допомогою паролів, створенню,

зберіганню та захисту яких не завжди приділяють належної уваги. В наших тезах ми розглянемо питання, які якраз і пов'язані зі створенням надійних паролів, їх збереженням та захистом, що по суті є одним із ключових питань кібербезпеки.

Надійні паролі мають відповідати наступним вимогам:

1. мінімальна довжина паролю 8 символів, максимальна 128
2. допустимі символи: [a-z, A-Z], [а-я, А-Я], [0..9]
3. як мінімум одна велика й одна мала літери
4. лише латинські і кириличні літери
5. як мінімум одна цифра
6. лише арабські цифри
7. без пробілів
8. спеціальні символи: ~ ! ? @ # $ % ^ & * =_ - + ( ) [ ] { } > < / \ | " ' . , : ; [2].

Для генерації надійних паролів та їх збереження варто використовувати менеджери паролів. Програмні засоби даного типу дозволяють оптимізувати створення та збереження даних входу (логінів та паролів), як локально (на жорсткому диску, флеш-накопичувачу тощо) так і у хмарі (дані зберігаються на веб-сервері та доступні з будь-якого пристрою, який має доступ до мережі Інтернет). Як і інші програми вони можуть бути безкоштовними (KeePass, Roboform, Sticky Password) та платними (Dashlane, NordPass) [3]. Більшість сучасних браузерів дозволяють зберігати дані входу до сайтів та інших онлайн ресурсів а також здійснювати генерацію паролів.

Для генерації паролів також можна використовувати веб-ресурси такі як Random.org, Passwords Generator, RandPass. Дані сервіси є досить простими для використання та надають змогу створювати паролі в залежності від обраних налаштувань користувачем [4].

Розглянемо способи за допомогою яких зловмисники можуть отримати дані входу користувачів (логіни та паролі).

Використання Keylogger (кейлоггер) – програмного забезпечення, або пристрою, який реєструє різні дії користувача, наприклад натискання клавіш на клавіатурі комп'ютера, рух та натискання кнопок мишки і так далі. Будь-яка інформація, яка вводиться користувачем надсилається зловмиснику, або записується на пристрій, який фізично приєднаний до комп'ютера. У випадку використання апаратного кейлоггера запис натиснутих клавіш буде йти лише до того часу, поки користувач фізично не від'єднає його від комп'ютера. Таким апаратним кейлогером може бути навіть звичайна флешка зі спеціальною мікросхемою, яка буде надсилати інформацію зловмиснику на електронну пошту.

Програмні кейлогери за способом зараження пристрою користувача не відрізняються від більшості іншого шкідливого програмного забезпечення. Вони потрапляють на комп'ютер за допомогою програми,

які завантажує з неперевірених джерел та встановлює користувач. Після відкриття, вони реєструють певну кількість натиснутих клавіш і надсилають інформацію зловмиснику на електронну пошту, це відбувається допоки вони не будуть видалені з комп'ютера [5].

Іншим способом заволодіння логіном та паролем користувача є фішинг – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів логінів та паролів шляхом надсилання електронного листа із пропозицією підтвердити реєстрацію облікового запису ввівши свій логін та пароль після переходу за посиланням, яке насправді є посиланням на сайт, зовнішній вигляд якого повністю копіює дизайн оригінального сайту. Є декілька ознак, на які потрібно звертати увагу і які свідчать про підроблений сайт: назва компанії з помилкою, неправильна url-адреса, підозрілі спливаючі вікна тощо. Навіть позначення безпечного сайту у вигляді заблокованого замка зліва від панелі URL-адреси браузера не може бути показником законності веб-сайту. Щоб убезпечити себе варто використовувати веб-браузер із виявленням антифішингу. Наприклад, Mozilla Firefox, який має безкоштовні доповнення (плагіни), які допоможуть виявити фішингові сайти [6].

Ще одним зі способів отриманні паролю є брутфорс (Brute force) – технологія, яка дозволяє підібрати будь-який пароль до аккаунту при наявності часу і бажання. Вона працює по принципу перебору можливих паролів, або груп символів з бібліотеки, яку використовує програма допоки пароль не буде підібраний [7]. Захиститись від даного методу допоможуть додатки Google Authenticator, Microsoft Authenticator, які генерують випадкові коди, які у поєднанні з основним паролем знижують ймовірність злому облікового запису зловмисниками [8].

Отже, безпеку використовуваних користувачем паролів забезпечує не складність пароля, зберігання його в надійному місці, використання захисту браузера, антивірусів та двофакторної авторизації а комплексне використання всіх цих заходів.

Список використаних джерел

1. Безпека в Інтернеті: що потрібно знати. *Профспілка працівників освіти і науки України*. URL: https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html
2. Вимоги до пароля. *Kaspersky Knowledge Base*. URL: https://support.kaspersky.com/KPC/1.0/uk-UA/183862.htm
3. Касунич К. 10 лучших менеджеров безопасных паролей 2021. *vpnMentor*. URL: https://ru.vpnmentor.com/blog/лучшие-менеджеры-безопасные-паролей/
4. Генераторы паролей: какие существуют и насколько безопасно их использовать – Сервисы на vc.ru. *vc.ru*. URL: https://vc.ru/services/48217-generatory-paroley-kakie-sushchestvuyut-i-naskolko-bezopasno-ih-

ispolzovat.
5. What is a keylogger? How attackers can monitor everything you type. *CSO Online*. URL: https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html
6. How Can I Identify a Phishing Website or Email? - Yahoo Safety. *Yahoo Safety – Home*. URL: https://safety.yahoo.com/Security/PHISHING-SITE.html?guccounter=1#:~:text=A%20phishing%20website%20.
7. Брутфорс. *Энциклопедия «Касперского»*. URL: https://encyclopedia.kaspersky.ru/glossary/brute-force/
8. Про двоетапну перевірку за допомогою програми для аутентифікації. *Kaspersky Knowledge Base*. URL: https://support.kaspersky.com/KPC/1.0/uk-UA/182858.htm

Роман Дідиченко

ЗМІСТ ТА СТРУКТУРА СОЦІАЛЬНОЇ КОМПЕТЕНТНОСТІ ПІДЛІТКІВ

На сучасному етапі розвитку суспільства дуже важливим при становленні особистості виступає формування соціальної компетентності. Підлітковий вік виступає одним з найважливіших періодів цього процесу. Але саме в цей віковий період особистість зіштовхується з рядом різних проблем, які можуть порушувати процес формування та розвитку соціальних компетентностей. Це визначає актуальність проблеми для наукового дослідження і практичної діяльності.

У працях таких науковців як: С. Бахтєєва, М. Гончарова-Горянська, Л. Лєпіхова, В. Слот, І. Зимня, Н. Бібік, С. Шишов, Л. Сохань, В. Сєріков, М. Рижаков, Р. Рогожніков, М. Нікандров, О. Овчарук, В. Краєвський, О. Крисан, В. Болотова, О. Бондаревська, Дж. Равен, Б. Рей та інших, поняття соціальної компетентності учнів визначається як специфічна здатність особистості, що дає змогу ефективно розв’язувати проблеми, в умовах реальних ситуацій життя. В дослідженнях цих та інших учених розкривається сутність поняття «соціальна компетентність» та визначаються її складові.

О. Пометун, вважає, що компетентність – це складна інтегрована характеристика особистості, під якою розуміють набір знань, вмінь, навичок, ставлень, що дають змогу ефективно діяти або виконувати певні функції, забезпечуючи розв’язання проблем і досягнення певних стандартів у галузі професії або виді діяльності [2].

О. Крисан у своїх працях наголошує, що компетентності виступають своєрідними комплексами знань, умінь і навичок, які людина набуває у процесі навчання й дозволяють їй розуміти та оцінювати ситуацію в різних